2006-12

The Department of Defense's transition of program of record (POR) systems from Internet Protocol Version Four (IPV4) to Internet Protocol Version Six (IPV6)

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

JOINT APPLIED PROJECT

The Department of Defenses Transition of Program of Record (POR) Systems from Internet Protocol Version Four (IPv4) to Internet Protocol Version Six (IPv6)

By: **Kyle L. Perkins and**
Michael A. Scott
December 2006

Advisors: **Raymond E. Franck and**
Brad R. Naegle

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2006	**3. REPORT TYPE AND DATES COVERED** Joint Applied Project	
4. TITLE AND SUBTITLE: The Department of Defenses Transition of Program of Record (POR) Systems from Internet Protocol Version Four (IPv4) to Internet Protocol Version Six (IPv6)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kyle L. Perkins and Michael A. Scott			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this report are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The objective of this Joint Applied Project was to examine the technical, financial, and implementation aspects for DoD transitioning POR systems to IPv6. The research outlines the initial intended useful life and limitations of IPv4 and IPv6. The financial aspects of transitioning to IPv6 are examined from a programs perspective, relative to the Program Objective Memorandum (POM). Implementation of transition strategies and mechanisms are identified and courses of action for implementing the mandatory IPv6 requirement are recommended. The principal finding of this research is that DoD Global Information Grid (GIG) assets must function in a dual IPv4/IPv6 capacity when transitioning to IPv6 in order to maintain the relevance of currently fielded programs. Furthermore, legacy GIG assets should be transitioned using Technology Refresh or Software Block upgrade programs while paying careful attention to the effects the transition has on tactical network operations.

14. SUBJECT TERMS IPv4, IPv6, Global Information Grid (GIG) Assets, Legacy GIG Assets, Transition Strategies, Tactical Network Operations			**15. NUMBER OF PAGES** 89
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE DEPARTMENT OF DEFENSES TRANSITION OF PROGRAM OF RECORD (POR) SYSTEMS FROM INTERNET PROTOCOL VERSION FOUR (IPV4) TO INTERNET PROTOCOL VERSION SIX (IPV6)

Kyle L. Perkins, BMD System Acquisition Specialist, PM Distributed Common Ground System - Army (DCGS-A) PEO Intelligence, Electronic, Warfare, and Sensors (IEW&S)

Michael A. Scott, Chief Engineer, PM Future Combat Systems (FCS) Brigade Combat Team (BCT), Warfighting Systems Integration Integrated Product Team (WFS IPT)

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN PROGRAM MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Authors:

_____
Kyle L. Perkins

_____
Michael A. Scott

Approved by:

_____
Raymond E. Franck, Ph.D, Lead Advisor

_____
Brad R. Naegle, Support Advisor

_____
Robert N. Beck, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

THE DEPARTMENT OF DEFENSES TRANSITION OF PROGRAM OF RECORD (POR) SYSTEMS FROM INTERNET PROTOCOL VERSION FOUR (IPV4) TO INTERNET PROTOCOL VERSION SIX (IPV6)

ABSTRACT

The objective of this Joint Applied Project was to examine the technical, financial, and implementation aspects for DoD transitioning POR systems to IPv6. The research outlines the initial intended useful life and limitations of IPv4 and IPv6. The financial aspects of transitioning to IPv6 are examined from a programs perspective, relative to the Program Objective Memorandum (POM). Implementation of transition strategies and mechanisms are identified and courses of action for implementing the mandatory IPv6 requirement are recommended. The principal finding of this research is that DoD Global Information Grid (GIG) assets must function in a dual IPv4/IPv6 capacity when transitioning to IPv6 in order to maintain the relevance of currently fielded programs. Furthermore, legacy GIG assets should be transitioned using Technology Refresh or Software Block upgrade programs while paying careful attention to the effects the transition has on tactical network operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AOL	America Online
APL	Approved Product List
ARP	Address Resolution Protocol
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
ASD NII	Assistant Secretary of Defense for Networks and Information Integration
BER	Bit Error Rates
BFAs	Battle Field Functional Areas
C2	Command and Control
CDR	Critical Design Review
CHS	Common Hardware / Software
CIO/G-6	Chief Information Officer, Deputy Chief of Staff
COCOMO	Constructive Cost Model
COTS	Commercial Off-The-Shelf
CT	Cipher Text
CTSF	Central Technical Support Facility
CY	Calendar Year
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information System Agency
DISN	Defense Information System Network
DISR	DoD IT Standards Registry
DITO	DoD IPv6 Transition Office
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DNS	Domain Name Service
DoD	Department of Defense
EPROMs	Electronically Programmable Read Only Memory
FCS	Future Combat System
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
FY	Fiscal Year
GIG	Global Information Grid
GOTS	Government Off-The-Shelf

HAIPE	High Assurance IP Encryption
HAG	High Assurance Guards
HIDS	Host-based Intrusion detection Systems
HQDA	Headquarters – Department of the Army
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICE	Independent Cost Estimate
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
IMA	Installation Management Activity
INE	In-line Network Encryptor
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISEC	Information Systems Engineering Command
ISP	Internet Service Providers
IT	Information Technology
ITES	Information Technology Enterprise Solutions
ITPWG	IPv6 Transition Plan Working Group
ITTF	IPv6 Transition Task Force
JC2	Joint Command and Control
JITC	Joint Interoperability Test Center
JTA	Joint Technical Architecture
JTA-A	Joint Technical Architecture – Army
JTRS	Joint Tactical Radio System
JTT	Joint Tactical Terminal
JWICS	Joint Worldwide Intelligence Communications System
LIR	Local Internet Registry
M&S	Modeling and Simulation
MACOM	Major Command
MIL NIC	Military Network Information Center
MS ELA	Microsoft Enterprise License Agreement
MTU	Minimum Transmission Unit
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization
NETCOM	Network Engineering Technology Command
NIDS	Network Intrusion Detection System

NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NIR	National Internet Registry
NIST	National Institute of Standards and Technology
NRO	Number Resource Organization
NSA	National Security Agency
NSS	National Security Systems
NTP	Network Time Protocol
OIF	Operation Iraqi Freedom
OMB	Office of Management and Budget
OPSEC	Operational Security
OSD	Office of the Secretary of Defense
OSD NII	Office of the Secretary of Defense for Network and Information Infrastructure
P3I	Pre-Planned Program Improvement
PDAs	Personal Digital Assistants
PDR	Preliminary Design Review
PEO	Program Executive Office
PEO C3T	PEO Command Control Communication Tactical
PKI	Private Key Infrastructure
PM	Program Manager
PMOs	Program Management Offices
POC	Point of Contact
POM	Program Objective Memorandum
POR	Program of Record
QoS	Quality of Service
RIR	Regional Internet Registries
RCIO	Regional Chief Information Officer
RFC	Request for Comments
SEND	Secure Neighbor Discovery
SME	Subject Matter Expert
SMF	Simplified Multicast Forwarding
SMTP	Simple Mail Transfer Protocol
SIPRNET	Secret IP Router Network
SWB	Software Blocking
SWBIA	Software Blocking Information Architecture
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Technical Integration Center

VoIP	Voice over IP
VPN	Virtual Private Network
WIN-T	Warfighter Information Network – Tactical

I. GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY JOINT APPLIED PROJECT PLAN

A. TENTATIVE PROJECT TITLE

The Department of Defenses transition of Program of Record (POR) systems from Internet Protocol Version Four (IPv4) to Internet Protocol Version Six (IPv6).

B. PROJECT PLAN ABSTRACT

The objective of this project is to examine the technical, financial, and implementation aspects for the DoD transitioning POR systems to IPv6. The technical aspects will be examined to establish a basis for the transition. The discussion will outline the initial intended useful life and its limitations. The financial aspects of transitioning will be discussed from a program's perspective relative to the Program Objective Memorandum (POM). Implementation of the transition will be discussed to identify the courses of action for implementing the mandatory IPv6 requirement. As a result of this project, officials in the Army will better understand whether or not the mandatory transition makes good business sense and is executable.

C. PROJECT SPONSOR

N/A

D. PROJECT TEAM MEMBERS

Name	Curric	Grad Date	Service	Signature	Date
Kyle Perkins	836	12/06	Army		
Michael A. Scott	836	12/06	Army		

E. ADVISOR

Name	Advisor Role/Org.	Approved	Date
Raymond E. Franck P.H.D	Lead Advisor/NPS		

F. ACADEMIC ASSOCIATE

Name	Curriculum	Reviewed	Date
Brad R. Naegle	836		

Submit completed Project Plan to the BPP Office of Instruction (IN306). Date_____

G. PROJECT DESCRIPTION

1. Project Title

The Department of Defenses transition of Program of Record (POR) systems from Internet Protocol Version Four (IPv4) to Internet Protocol Version Six (IPv6).

2. Project Topic

Analyze and compare IPv4 and IPv6, while outlining the business case for implementation.

3. Project Objectives

To determine the need and direction for IPv6, based upon answers to the following four questions:

Q1: How should address space be allocated?

Q2: How does the DoD's financial system bound the implementation?

Q3: What are the benefits's for the DoD to transition to IPv6?

Q4: What are the issues surrounding the transition to IPv6?

Q5: What are the transition mechanisms and strategies regarding IPv6?

4. Background

The DoD has established the goal of transitioning all DoD networking to the next generation of the Internet Protocol, IPv6, by Fiscal year (FY) 2008. A key tenet of the DoD transition strategy is to minimize later transition costs by ensuring that the products and systems that are procured, acquired or in development after 1 October 2003 are capable of operating in IPv6 networks, as well as maintaining a capability to operate in today's IPv4 world. Given DoD's generally long technology refreshment cycle and lengthy development timelines this direction is intended to posture DoD to complete a transition to IPv6 by 2008 with minimal additional cost and impact to current capabilities.

H. ACTIVITIES

1. Problem Identification

The IPv4 to IPv6 transition will be a significant challenge for the Army. A large number of hardware and software systems including applications will need to be upgraded or replaced, in some cases under an accelerated technology refresh rate. During

the transition phase, new or modified IPv6 capable systems and applications will need to operate with the existing IPv4 systems and applications without degradation in performance, reduction in availability, or compromise of security. Application migration to IPv6 is a complex and difficult area of transition. Business and institutional system migrations are dependent on commercial vendors support. We must get industry partners (not just defense contractors) working to help meet the Army's goals.

2. Appropriate Data

Data will be collected from Army Program Management Offices (PMOs) which manage the weapons systems and various other DoD organizations that have a significant interest in the transition.

3. Appropriate Analysis

Reports and information will be analyzed to determine feasibility, if any, based upon the finalized project objectives list.

I. EXPECTED ACCOMPLISHMENTS

1. Product

Joint Applied Project Report.

2. Report Content

An analysis sufficient to determine whether or not the DoD's strategy for implementing IPv6 across DoD networks is viable. Evidence sufficient to determine whether or not the DoD's mandates are being implemented effectively to affected programs.

J. ROLES OF PROJECT PARTICIPANTS

1. Role of Team Members

There are both collective and individual roles for team members. Collectively, the members will develop the final project schedule and plan of activities (including assignment of individuals to activities), further develop the research methodologies, peer review the data and analysis, review and comment on the final report draft to form a consensus version. Individually, team members will perform research/gather data in independent areas in parallel (to speed data gathering efforts), perform data analysis in parallel using common agreed-upon methods, and develop drafts of specific sections of the final report. One team member will be designated as the final version editor/tech

writer. Research tasks will be split based on individual expertise, organizational element, and interest. Team members are also expected to participate in regular group meetings to assess progress, discuss and/or correspond with the advisors telephonically or through email on a regular basis, and to perform all tasks IAW the agreed-to schedule. Since the team members are not collocated together the use of email and telephone is expected to be the norm.

2. Role of Advisors

The project advisors are expected to provide guidance to the team on:

- Scope and expected timeframe of efforts to enable completion.
- Data sources and gathering methods, including identifying pertinent POCs and known related studies.
- Report writing/style and content.

The advisors are also expected to be available for periodic planned telephonic discussions of project status, and be available to answer email and impromptu telephone questions in a mutually-agreed-to timeframe.

K. SPONSORS/CLIENTS

None.

L. OTHER

None

M. SCHEDULE

(all dates CY06 unless otherwise noted)

Jun-Jul	Initial project plan, secure advisors. [Completed]
Aug-Sep	Finalize project plan – gain approval of advisors and associate.
	Develop detailed schedule, assign individual tasks (research, analysis).
Sep	Begin individual research tasks, including info gathering DoD programs affected by IPv6 transition.
Oct	Complete individual research tasks. Begin data analysis. Begin writing report (background, approach, etc.).
Nov	Complete data analysis. Develop conclusions
Nov-Dec	Submit “chapters” to advisors as available for review.
Early Dec	First draft of full report, submit to Advisors for comments/revisions.

Mid Dec Receive comments/revisions, incorporate, finalize report.

Mid Dec Advisor(s) approval of report. Begin submittal process for NPS approval.

Jan/Feb 07 Report published by NPS.

N. RESOURCES

No additional resources or funding anticipated.

O. REFERENCES

P. SECURITY CLASSIFICATION

Unclassified.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IPV6 BACKGROUND

A., IPV6 INTRODUCTION

The internet currently operates under IPv4 which was developed in the 1970's. IPv6 was designed to support continued Internet growth in number of users and functionality and is the next generation of Internet protocol. The growth of the Internet is currently constrained due to the limitations that IPv4 suffers from. IPv4 allows for only 2^{32} (4,294,967,296) addresses which seems like a very large number, but in fact is much too small for today and tomorrow's Internet.

The population of the Earth has grown to approximately 6.6 billion people and with IPv4 there is not enough address space available to give one IP address to every person on the Earth. IPv6 has been under development for over ten years and has been designed to overcome these limitations by greatly expanding available IP address space, and by incorporating other features such as mobile communications, Quality of Service (QoS), end-to-end security, and system management burden reduction. The rapid growth of the Internet as a fundamental technology for commercial, social activity, and military information transfer has been staggering. The Internet has grown rapidly in the past five years to a level well beyond that which the original Internet designers envisioned over twenty years ago.

Global IP address space is now at a premium and applications are forced to work with mechanisms that provide local addressing. Without sufficient IP addresses numerous workarounds such as Network Address Translation (NAT) and extensions to IPv4 have been implemented to try to overcome its limitations. These workarounds allow multiple devices to use local private addresses within an enterprise while sharing one or more global IPv4 addresses for external communications. While NAT has delayed the exhaustion of IPv4 addresses it also complicates the application of general bi-directional communication. IPv6 removes the need for the use of NAT since global addresses will be widely available.

The transition of the global Internet from IPv4 to IPv6 is expected to span many years. During this period, many organizations will introduce IPv6 into their infrastructure and will operate in a dual stack environment supporting IPv4 and IPv6 concurrently. The incremental approach allows for a period where IPv4 and IPv6 can co-exist using one or more transition mechanisms to ensure interoperability between the old and new protocols. The transition to IPv6 is expected to be complicated and the transition strategies for IPv6 will be dependent on the networks and systems targeted for transition.

B. IPV6 FEATURES AND BENEFITS

The design and evolution of the IPv6 protocol represents the work of many Internet Engineering Task Force (IETF) and working group proposals over several years. The core of IPv6 was built on the existing features of IPv4 and designed to provide new services and capabilities. The driving requirement for IPv6 was to extend the IP address space enough to offer a unique IP address to any device. IPv6 was also designed to enable stateless IP auto-configuration and improved "plug and play" support, provide support for network address renumbering, enable mandatory implementation of IP Security (IPsec) support for all fully IPv6-compliant, and improve support for IP Mobility.

The following is a list of the features and benefits IPv6 is intended to provide:

- **Larger address space** – IPv6 increases the IP address size from 32 bits to 128 bits. Increasing the size of the address field increases number of unique IP addresses from approximately 4,300,000,000 (4.3×10^{9}) to 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}).
- **End-to-end transparency** – The increased number of available addresses reduces the need to use address translation technologies.
- **Hierarchical addressing** – The hierarchical addressing scheme provides for address summarization and aggregation. These approaches simplify routing and manage routing table growth.
- **Enhanced applications functionality** – Simplifies direct peer-to-peer applications and networking by providing a unique address to each device.
- **Scalability of multicast routing** – IPv6 provides a much larger pool of multicast addresses with multiple scoping options
- **Auto-configuration** – Clients using IPv4 addresses use the Dynamic Host Configuration Protocol (DHCP) server to establish an address each time they log into a network. This address assignment process is called stateful

auto-configuration. IPv6 supports a revised DHCPv6 protocol that supports stateful auto-configuration, and supports stateless auto-configuration of nodes. Stateless auto-configuration does not require a DHCP server to obtain addresses. Stateless auto-configuration uses router advertisements to create a unique address. This creates a "plug-and-play" environment, simplifying address management and administration. IPv6 also allows automatic address configuration and reconfiguration. This capability allows administrators to re-number network addresses without accessing all clients.

C. DOD IPV6 TRANSITION

The Department of Defense has established a goal that all Global Information Grid (GIG) Information Technology (IT) assets are to transition from the current Internet Protocol Version 4 (IPv4) to the newly developing Internet Protocol Version 6 (IPv6) by FY08 in order to avoid technical obsolescence within the next 10 to 20 years. Although the transition to IPv6 is currently progressing rapidly in Asia and Europe, its acceptance in North America has been minimal. Nonetheless, the eventual ubiquitous implementation of IPv6 seems to be inevitable, and the long development cycle of technology in the defense industry has prompted the DoD to become an early advocate of implementing IPv6.

In response to the DoD goal and subsequent guidance, the Army has established a transition plan to facilitate a well-coordinated effort to phase-out IPv4 and replace it with IPv6. The task is very extensive and complex because it impacts tens of thousands of computing and communications devices, and software applications.

The Army plan provides a governance structure that will be headed by the Chief Information Officer, (CIO/G-6). A working group and a task force have been formed to assist the CIO/G-6 in planning and managing this mission. The plan also provides detailed guidance to the organizations that will be implementing IPv6 in their products and systems. The IPv6 implementers include the twelve Program Executive Offices (PEOs), the Installation Management Activity (IMA), the Major Commands (MACOMs), the Army Reserve, and the National Guard Bureau.

It is expected the full transition to IPv6 will take many years, and during the interim the two IP protocols will co-exist. The transition is also expected to be quite

costly. Senior leaders in the DoD hope additional costs can be controlled by implementing IPv6 through the normal technical refresh cycle of a program or through pre-planned product improvements (P3I). However, costs will be incurred to mitigate risk through the establishment of pilot programs and testing. A waiver process is available for cases in which systems may not be able to transition in a timely manner, or where systems may never be able to transition due to severe technical, logistical, or financial restrictions.

To maintain secure operations, it is clearly stated in the DoD and Army transition plans that IPv6 is not be used on any operational network, or any DoD network carrying sensitive information, until it is completely compliant with all National Security Agency (NSA) requirements. (Department of the Army Internet Protocol Version 6 (IPv6) Transition Plan (Phase 1) Version 0.9, 11 March 2004)

1. Army IPv6 Transition

On 9 June 2003, the Assistant Secretary of Defense for Networks and Information Integration (ASD NII) issued a policy memorandum regarding the Enterprise-wide deployment of IPv6. The policy establishes the goal of transitioning all DoD enterprise-wide networks from IPv4 to IPv6 by Fiscal Year (FY) 2008. The policy pertains to all IT and National Security Systems (NSS) which make up the GIG. Key points of this policy include the following:

- As of October 1, 2003, all GIG assets being developed, procured, or acquired shall be IPv6 capable, in addition to maintaining interoperability with IPv4 systems and services.
- Specific near-term IPv6 implementation pilots, demonstrations, and test beds will be identified by the DoD Chief Information Office (CIO) as part of the transition planning process.
- No implementations of IPv6 shall be permitted on the networks carrying operations traffic within the DoD until authorized by the DoD. This is to assure that all information assurance concerns have been properly addressed prior to implementing IPv6.
- The DoD CIO will lead, in consult with the Joint Staff and with the participation of the DoD Components and Services, the development of an IPv6 transition plan.

On 29 September 2003, the ASD NII issued a related memorandum to provide interim guidance to support the requirement to begin to procure and acquire IPv6-capable GIG assets on 1 October 2003. The memorandum defines the meaning of IPv6 capable, announces a Joint Technical Architecture (JTA) standards profile for IPv6, and describes a waiver process. These issues will be discussed in more detail in the following sections. In response to the DoD memorandums, the Army CIO, LTG Boutelle, issued a memorandum on 5 November 2003, endorsing the Army's position to support the transition to IPv6. (Department of the Army Internet Protocol Version 6 (IPv6) Transition Plan (Phase 1) Version 0.9, 11 March 2004)

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOD TRANSITION OF PROGRAM OF RECORD (POR) SYSTEMS FROM IPV4 TO IPV6

A. HOW TO ALLOCATE ADDRESS SPACE? WHAT IS AN INTERNET PROTOCOL (IP) ADDRESS?

As the Department of Defense (DoD) moves further into the digital arena of warfare, the demand for Internet Protocol (IP) address space is increasing dramatically. The future theater of operations will require manned and unmanned ground vehicles, air vehicles, sensors and munitions to have networked suites of weapons interoperating seamlessly with other military networks. In order for these devices to receive information and communicate, they will require IP addresses. An IP address identifies and allows these devices to communicate with each other. This means all devices from Personal Digital Assistants (PDAs) to Command and Control Suites that require a connection to the internet will also need an IP address. This can be thought of as a street address or phone number because an IP address identifies a specific computer or computer device that is connecting to the internet.

B. CURRENT WORLDWIDE SPACE ALLOCATION

The Internet Assigned Numbers Authority (IANA) is the global body that allocates super-blocks of address space to Regional Internet Registries (RIR), who then allocate smaller blocks to Internet Service Providers (ISP) and enterprises. An ISP such as America Online (AOL) will then charge a fee for using one of their IP addresses to connection to the internet. ISPs obtain allocations of IP addresses from a local Internet registry (LIR) or national Internet registry (NIR), or from their appropriate Regional Internet Registry (RIR):

- AfriNIC (African Network Information Centre) - Africa Region
- APNIC (Asia Pacific Network Information Centre) - Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) - North America Region
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) - Europe, the Middle East, and Central Asia

C. ALLOCATION PRINCIPLES

The IANA will allocate sufficient IPv6 address space to the RIRs to support their registration needs for at least an 18 month period. The IANA will also allow the RIRs to apply their own chosen allocation and reservation strategies in order to ensure the efficiency of their work. The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the global coordination of the Internet's system of unique identifiers. Unique identifies include domain names like .org or .museum, and country codes such as .UK .IE. Any new RIR shall, on recognition by ICANN receive an IPv6 allocation from the IANA. A RIR is eligible to receive additional IPv6 address space from the IANA when either of the following conditions is met: the RIR's available space of IPv6 addresses is less than 50% of the minimum number of allocated address spaces or the RIR's available space of IPv6 addresses is less than its established necessary space for the following 9 months. In either case, IANA shall make a single IPv6 allocation, sufficient to satisfy the established necessary space of the RIR for an 18 month period.

If the applying RIR anticipates that more address spaces will be required within a six month period actual space allocated will be determined by calculating total needs according to a projection and special facts that justify these needs. When additional necessary space is required, RIR's are required to submit a clear and detailed justification with the above mentioned projection. If the justification is based on the allocation tendency prepared by the RIR's data, explaining said tendency must be enclosed. If the justification is based on external factors such as a new infrastructure, new services within the region, technological advances or legal issues, the corresponding analysis must be enclosed together with references to information sources that will allow verification of the data. If IANA does not have elements that clearly question the RIR's projection, the special needs projected for the following 18 months, indicated above, shall be considered valid. The IANA, the NRO, and the RIRs will make announcements and update their respective web sites regarding an allocation made by the IANA to an RIR. ICANN and the Number Resource Organization (NRO) will establish administrative procedures to manage this process.

D. ADDRESSING PLAN FOR THE DOD

Addressing plans are constrained by The Office of the Secretary of Defense for Network and Information Infrastructure (OSD NII), which has directed the DoD to incorporate IPv6 and operate in a dual IP (IPv4 and IPv6) capacity for the foreseeable future. OSD NII further directed that IPv6 be deployed principally utilizing existing technical refresh funding. The current communication model of the DoD is similar to that of a corporate holding company and not a single enterprise. Relationships exist between IP (IPv4 and IPv6) address block allocation, the Domain Name System (DNS) system, routing, and certain Information Assurance (IA) capabilities that are mission essential to the DoD. Relationships exist between IP (IPv4 and IPv6) address block allocation, the Domain Name System (DNS) system, routing, and certain Information Assurance (IA) capabilities that are mission essential to the DoD.

ARIN has allocated four IPv6 address prefixes for the DoD's use. The DoD IPv6 Transition Office (DITO), Defense Information Systems Agency (DISA), and the representative Services (Army, Navy and the Air Force) have consensus on the initial high-level IPv6 address allocation process Addressing Plan. The DoD is planning for the reassignment of these address blocks among the Services, Agencies, and other DoD organizations. The Military Network Information Center (MIL NIC) will reassign the GIG CT Core IPv6 address blocks between, unclassified, secret, and the top secret address block to the USN NIC for its address reassignment function. The GIG is a globally-connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand. The MIL NIC will reassign the GIG CT Core IPv6 address block, the unclassified IPv6 address block, secret IPv6 address block, and the top secret IPv6 address block to the MIL NIC for its address reassignment function. The MIL NIC will reassign the GIG CT Core IPv6 address block, the unclassified IPv6 address block, secret IPv6 address block, and the top secret IPv6 address block to the AF NIC for its address reassignment function. The MIL NIC will reassign the GIG CT Core IPv6 address block, the unclassified IPv6 address block, secret IPv6 address block, and the top secret IPv6 address block to the ARMY NIC for its address reassignment function. The MIL NIC

will retain the remaining IPv6 address space for its own address reassignment function to joint programs and for future use by the service NICs.

E. NETWORKS

DoD's Unclassified and Classified traffic are transported over completely segregated networks, such that each level of classification has its own separate infrastructure, network services, and administration. IPv6 addressing plans are expected to support this architectural choice in the short term, and as long as such networks segregated by classification levels exist. DoD programs will only connect to peers with IPv6 address space of the same classification. Unclassified, Allied and Coalition programs may connect with non-DoD entities through approved IA access points. Allied and Coalition networks will be appropriately segregated from operational DoD networks of similar classification.

After 2008 the DoD will introduce the Global Information Grid (GIG), also known as the Black Core or Cipher Text (CT) Core architecture. The GIG CT will have dedicated infrastructure, network services, and administration. In the CT Core architecture, all Plain Text (PT) traffic will be encrypted using High Assurance Internet Protocol (HAIPE) Devices, and the encrypted packet will be appended with the IPv6 address of the destination HAIPE Device. The destination HAIPE Device, once having received the encrypted packet, decrypts it, and then forwards it to the destination host.

F. DOD NETWORK INFORMATION CENTER IPV6 ADDRESS MANAGEMENT

The Department of Defense (DoD) maintains the MIL NIC, Service NICs, and Agency NICs organized in a hierarchical structure. These are collectively termed "DoD NICs". DoD NICs will function similarly with IPv6 since they do with IPv4. The MIL NIC, as part of the Defense Information Systems Agency (DISA), will manage the ongoing acquisition of IPv6 address space for the entire Department of Defense (DoD) and its reassignment within the DoD enterprise.

Figure 1 illustrates the relationships between the DoD NICs, RIRs, and IANA. The MIL NIC shall manage the reassignment of IPv6 address blocks to Service NICs, Agency NICs, and directly to appropriate joint programs based upon demonstrated need.

Service and Agency NICs will acquire IPv6 address blocks solely from the MIL NIC and will reassign IPv6 address blocks only to their respective Service and Agency programs according to demonstrated need.

DoD NICs will continue to maintain Domain Name Servers (DNS), zone files, and delegate subordinate zones for their respective forward DNS zones. The DNSs translates web addresses such as "http://www.nps.navy.mil" into an IP address so the computer can communicate on the network. Zone files store and categorize the DNS information. For example, the MIL NIC will continue to maintain DNS servers for the MIL forward DNS zone and delegate subzones of .mil to the DoD Services and Agencies. In another example, the Navy NIC will continue to maintain DNS servers for the NAVY.MIL forward DNS zone.

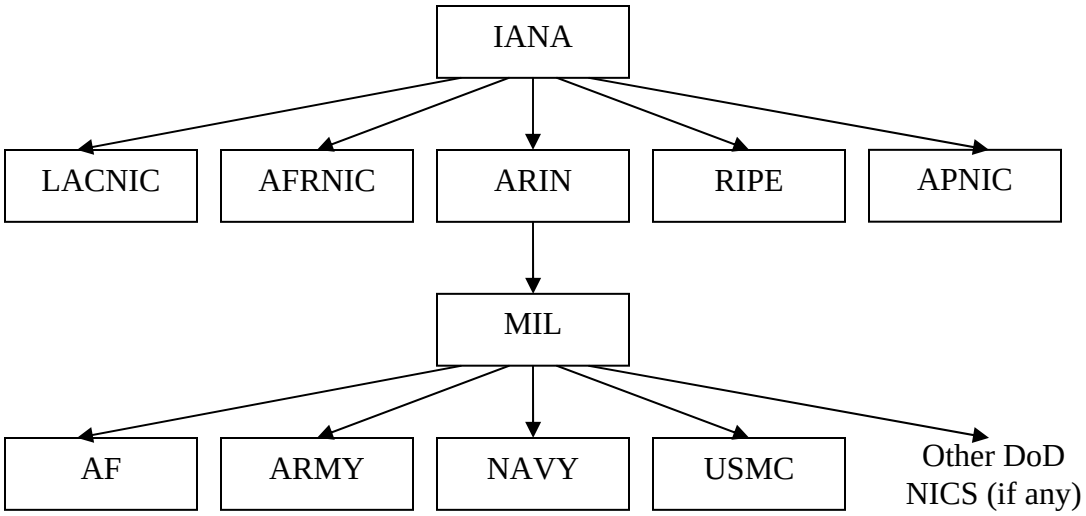

Figure 1. Relationships between the DoD NICs, RIRs and IANA (From: Brig, P. Michael and Cansever, Derya)

G. DOD COST TO TRANSITION POR SYSTEMS FROM IPV4 TO IPV6

The Department of Defense has established a goal that all GIG IT assets are to transition from the current IPv4 to the newly developing IPv6 by FY08 in order to avoid technical obsolescence within the next 10 to 20 years. In order to meet this date the DoD issued a mandate dated 9 Jun 2003. Although the transition to IPv6 is currently progressing rapidly in Asia and Europe, its acceptance in North America has been minimal. Nonetheless, full implementation of IPv6 seems to be inevitable, and the long development cycle of technology in the defense industry has prompted the DoD to become an early advocate of implementing IPv6. (DEPARTMENT OF THE ARMY INTERNET PROTOCOL VERSION 6 (IPv6) TRANSITION PLAN (Phase 1) Version 0.9 dated 11 March 2004)

H. OVERALL DOD ESTIMATE TO MEET MANDATE

The DoD has estimated that in order to meet the FY08 mandate $2.3B additional funding would be required (Director, Technical Architecture Division Architecture Operations Network & Space CIO/G-6). This estimate was based on the assumption that all GIG IT assets will be transitioned regardless of where these assets are in their lifecycle (i.e. Development, Deployed, within 5 years of obsolescence). The current DoD transition estimate makes some overriding assumptions and extends the transition period until FY16, which reduces the transition cost by approximately 50% or $1.6B (Director, Technical Architecture Division Architecture Operations Network & Space CIO/G-6). The assumption was made to reduce the cost to DoD center on the basic principle that the transition will be implemented with Technology Refresh whenever feasible. The majority of the cost estimate includes:

- Experimentation, Testing, Modeling & Simulation
- Transition Mechanisms
- Pilots
- Certifications
- Programs without Tech Refresh or P3I
- Dual IP-Layer O&M (FY10-13)
- Training

The current estimate for transition costs centers on Technology Refresh while half the cost of the original estimate still represents a substantial investment for DoD and funding must be identified in the POM in order to implement the transition. The current POM funding identifies approximately $600M to implement the transition. While this funding is roughly half the current DoD estimate the funding is based on the assumption that the transition will align with current technology upgrade programs as the following:

- GIG Bandwidth Expansion
- Task Force Modularity
- LandWarNet Architecture
- Deployment of Enterprise-level Transition Mechanisms
- Fielding of JTRS and WIN-T

I. ARMY PROGRAM EXECUTIVE OFFICES (PEO) ASSUMPTIONS FOR TRANSITION COST ESTIMATES

The Army's nine PEOs have established an IPv6 Transition Plan Working Group to evaluate progress made on implementing the IPv6 Transition Plan. The working group allows PEOs to share information among members and provide additional guidance relevant to the transition.

CIO/G6 provided PEOs costing templates that provide a comprehensive set of issues to consider when developing transition cost estimates. While working the requirement many of the PEOs have experienced difficulty gathering the required information from PMs. PEOs are continually working with PMs to gain consistency on the reports in order for the requirements to be validated. Most of the problems PMs are having while attempting to gather the required information is the significant number of unknowns. PMs continually receive mixed guidance on IPv6 transition because most are slated for termination or replacement with the FCS.

PEO Command Control Communication Tactical (PEO C3T), headquartered at Ft. Monmouth, New Jersey expressed several concerns relative to the transition. First, systems deployed in support of Operation Iraqi Freedom (OIF) are granted blanket waivers that withdraw the requirement to transition system by FY08. This waiver will cover systems procured for immediate mission support and enhance the ability to support

the soldier in a timely manner. Another issue of concern is modularity is not being implemented with a normal Program Objective Memorandum (POM) cycle. Modularity changes the scope of the network infrastructure and PEO C3T has not been provided POM information which would allow them to identify technology refreshments. This information is based on the fact that the Army will not fund Common User System modifications after FY06. This significantly affects the ability for PEO C3T to fund the transition.

J. PM ASSUMPTIONS FOR TRANSITION COST ESTIMATES

- The DoD mandate applies to IP based systems and networks, only if a system/network is part/component of, or draw service from the GIG that systems must transition.
- If a system/network is not a part/component of, nor derives services from the GIG, system will not be required to transition to IPv6, however it, must transition to IPv6 when requirements change.
- Contractor-Government interface must be IPv6 capable.
- OSD is responsible for transition of joint programs.
- The SINCGARS/EPLRS network will not transition to IPv6. It will be replaced by IPv6-capable WIN-T and JTRS starting in about 2009. Waivers will be granted in the interim period.
- DoD will establish the minimum testing standards for IPv6 compliance.
- IPv6 capable COTS products will be available via acquisition or upgrade of new software. This includes networking products (routers, firewalls, net management tools, etc.), network services (directory services, DNS, etc.). Networked applications (email servers, C4 systems, databases, medical systems, etc.).
- Testing and certification (including security certification, accreditation, and safety critical testing) of systems not yet at Milestone C should not be included as part of the IPv6 transition.
- Systems within five years of obsolescence (from FY04) will not be required to transition to IPv6. The replacement system must be identified.
- Organizational Intranets will be transitioned by the owner using his own programmed resources and timeframes.
- IPv4 and IPv6 will coexist past the current POM (beyond FY11).
- Costs will be incurred to integrate multi-vendor (COTS) IPv6 capable products.

- If feasible to make GOTS products IPv6 capable, then costs will be incurred, otherwise, co-existence mechanisms will be used as interim solution until replacement.
- Expenses to upgrade HAIPE, INE, HAG will be borne by DoD.
- Additional costs may be incurred to mitigate IPv6 performance issues.
- Waivers will be granted for all systems developed in Software Blocks prior to the implementation. Rationale for this waiver is that supporting interoperability systems and radios will not be available until at least Block 4, 5, or 6. (Implementers IPv6 Transition Plan for PEO Ground Combat Systems)

K. BENEFIT TO THE DOD OF TRANSITION

1. Interoperability

Traditionally the DoD has administered data interoperability programs. Data administration attempted to standardize and control data elements, definitions, and structures across the DoD enterprise of databases and networks. This approach requires consensus among and across organizations, standardization of data elements, minimized duplication of data elements, and reduced need for data element translation. This approach has since been abandoned due to the vast scope of the DoD.

The Net-centric vision for the future of the DoD's fighting force depends significantly on the GIG providing interoperability of inter-networked sensors, platforms, facilities, people and information. This vision will connect everyone from the commander to the warfighter in the field and is founded on the principles of the GIG's transport layer. Increased interoperability will allow soldiers to leverage the same data, rather than relying on traditional point-to-point interfaces. Having soldiers connected across the spectrum of operation will accelerate decision cycles by having the data visible, available and usable when and where it is needed. The increase in speed in accessing data will further enhance the commander's decision making in situations where time is of the essence. Data will be available so users can receive information in a timely manner without waiting for processing, exploitation, and dissemination. With data posed to shared spaces the user can determine the utility of information rather than waiting for the originator to process.

The Net-centric Data Strategy seeks to expand the focus of visibility and accessibility of data rather than just standardization. The strategy recognizes the need for data to be available for unanticipated users as well as the originally intended users. The overall objective is to increase the ability of the system to leverage the same data without the ability to access the information to be designed in. The Net-centric strategy will realize the availability of system files, databases, documents, official electronic records, images, audio files, web sites, and data access service. This significantly moves the culture away from processing, exploiting, and disseminating to a post before process mentality.

2. Improved End-to-End Security

The security of DoD networks is essential to successfully implementing IPv6. Several steps must be taken to ensure that classified information is not compromised during the transition. While the commercial world and DoD evolve to IPv6 DoD will continue to leverage work in this area and take advantage of products that emerge.

The security issues surrounding transitioning to IPv6 start with the transition mechanisms themselves because IPv6 products can create potential vulnerabilities due to their immaturity. Intrusion Detection Systems (IDS) generally detect unwanted manipulations to systems and is often referred to as an Anti-Virus application. These systems are categorized as: Host-based and Network-based. Host-based Intrusion detection Systems (HIDS) consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state. A Network Intrusion Detection System (NIDS) is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. Thus far, little has been accomplished to establish IDSs for IPv6 due to lack of demand. In order for IDSs to mature industry must establish rules against detection of what is known to be bad to what is not explicitly allowed. This rule change will decrease the rules that need to be applied against every system request.

Additional security concerns for IPv6 include features such as Secure Neighbor Discovery (SEND), Quality of Service (QoS), address auto configuration, and mobile IP.

SEND is a protocol that allows users to access domains while simultaneously securing the domain. SEND is like the mail slot in a storefront. Individuals can deliver mail to the mail slot but only the store owner can open the door and read the mail. QoS is the capability of a network to provide better service to selected network traffic by prioritizing the request for information. When requests are classified with higher priority QoS seeks to improve the flow of information. Address auto configuration creates a link-local address and verifies its uniqueness on a link, then determines what information should be auto configured. Mobile IP enables a router on a user's home subnet to intercept and transparently forward IP packets, or information to users while they travel beyond network boundaries. The security of this technology is essential to soldiers who will be operating with PDAs.

Another significant issue surrounding the DoD's security posture while fielding IPv6 is the widespread use of end-to-end IPSec. IPSec establishes security over a network between a single sender and a single receiver. This capability is useful when only trusted computers are allowed to access a server. IPSec acts as a control for accessing applications and services running on the server. The system will either encrypt or authenticate the traffic, depending on required level of security.

Established policies and processes the DoD currently uses also have an impact on implementing IPv6. The Defense Information Systems Network (DISN) has security provisions as well as connection approval processes for connecting to all DISN networks and the network interconnections among them. In addition to these requirements all other networks within DoD have System Security Authorization Agreements, which are required by the DoD Information Technology Security Certification and Accreditation process (DITSCAP).

3. Ease System Management Burdens

With the increase in address space that IPv6 brings one could imagine that managing an IPv6 network would require a significant increase in management resources. Fortunately, the designers of IPv6 recognized the limitations of IPv4 and implemented several improvements into IPv6.

IPv6 increases IP encryption from 32 to 128 bits. This increase avoids potential exhaustion of address space and vulnerability to malicious attack. Increasing the bits of the IP address also eliminates the need for Network Address Translation (NAT) and other devices that break the end-to-end nature of Internet traffic. Eliminating the need for NAT is significant because source and/or destination addresses of IP packets will not require rewriting as they pass through a router or firewall. Administrators will find managing the increase of address space easier since large blocks of address space can be allocated. This avoids fragmentation of the address space, which in turn leads to smaller routing tables.

Another feature that IPv6 offers is Auto-configuration of Nodes. Auto-configuration will automatically configure devices without manual intervention. This eliminates the need for software configuration programs or devices that close a break in a bypass to an electrical circuit. Auto-configuration replaces Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (ARP). DHCP allows computer devices to use rules to allow the device to request and obtain an Internet address from a server. This is essential because the server assigns the available addresses. ARP is a method of finding a host's hardware address when only its IP address is known. This is vital when two hosts are on the same network and one is required to send a packet to the other.

4. Unlimited Address Availability

Increasing the availability of address space is essential to the success of the DoD's vision for a digital battlefield. The concept of having every soldier and piece of equipment interconnected will require a significant amount of IP addresses. This is the primary reason the DoD is pushing for the implementation of IPv6 by 2008.

The 32 bit length of an IPv4 IP address has limited the available address space to $4.3X10^9$ addresses. This may appear to be a significant amount of address space until you consider every cell phone, PDA, car, etc. will require an IP address. This is where IPv6 shows its true potential as the address space solution for the next several decades. IPv6 has enough room for $3.4X10^{40}$ unique addresses. This increase in address space can

equate to addressing each square inch of the planet earth and will satisfy the world's requirements of IP addresses today, tomorrow, and into the foreseeable future.

Increasing the IP address size from 32 to 128 bits enhances applications transparency. Having significantly more transparency will alleviate the user from worrying about technical details such as: installing, updating, downloading, or installing device drivers. Increased transparency can allow users to compress data automatically, which enables more files to be stored without manual encryption. Transparency also establishes single uniform ways users perform individual computing. The most significant aspect of transparency, relative to DoD, is location transparency. Users will not be required to know where a single user is located. This enables the distributed architecture that DoD is striving to achieve. Under a distributed architecture users will have the ability to access, share, and collaborate among user across the spectrum of operation seamlessly.

L. ISSUES SURROUNDING DOD TRANSITION

Many systems that utilize IPv4 addresses directly will have to be recoded to handle IPv6. If the systems are old, this may no longer be feasible, and these systems will have to be replaced by newer models. Many systems applications were custom-written and the original writers are no longer available. New custom applications may have to be commissioned. Many of the older systems do not contain hardware designed for easy reprogramming (i.e. firmware, EPROMs, etc.). These systems will be very difficult to reprogram and test. Any reprogramming will be a lengthy process, with the need to test and debug any newly created software.

In the case of "disruptive" systems (those that can only work under IPv6), and which portend great benefits, there of course can be no "transition"; the new hardware and software must be put in all at once. Since everything is unlikely to work smoothly at first, a shakedown period must be allowed. Depending on the transition mechanism, this may include special tunneling/translation mechanisms to accommodate older systems that cannot transition. IPv6 will increase complexity, delay deployment, and impact performance of the IPv6 systems being fielded.

M. MAINTAINING INTEROPERABILITY

Program Managers (PMs) will need to ensure that the systems they manage maintain interoperability as they transition away from today's IPv4-only environment. During the initial phases of transition, PMs are likely to move to an environment that accommodates IPv6 in a largely IPv4 environment, which leads to an ever-present dual stack environment where systems can operate in both IPv4 and IPv6. As systems transition and the use of IPv4 diminish PMs will operate in an environment largely as an IPv6 network. Hardware and software interoperability will be essential as PMs move forward with their IPv6 plans and interconnect their systems across dual environments. Since maintaining interoperability and security for these types of evolving environments is the highest priority, the transition period should be minimized.

There are many possible combinations of technical IPv6 transition strategies. There are also a number of transition mechanisms (e.g. dual stack, tunneling, translation) which PMs can choose from with more emerging from the technical community. The introduction of IPv6 on an enterprise scale will introduce a number of challenges including scalability, integration, and security. In the near term, there is concern about creating vulnerabilities in existing IPv4 networks by deploying IPv6 and its transition mechanisms. (IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006)

N. SECURITY ISSUES

The DoD is required to conduct risk assessments and develop security plans in accordance with the Federal Information Security Management Act (FISMA) and as required by National Security Policy, OMB Policy, and in accordance NIST standards and guidance as necessary.

Several security implications of adopting IPv6 within a program are provided below as initial guidance to identify a network security infrastructure plan within each agency:

- Security applications infrastructure currently used on an IPv4 network will need to be replicated, with an expectation that the same level of assurance is provided in the IPv6 network. Examples of those applications are

Intrusion Detection, Firewalls, Network Management of IP Packets, Virus Detection, Intrusion Prevention, Secure Web Services Functions, etc.

- If end-to-end IPsec security is to be implemented, there will be a need to identify PKI, key management, and policy management infrastructures that meet the scalability and security verification requirements for intra-network communications (e.g. nodes, devices, and sensors).
- If end-to-end IPsec security is implemented, the current network perimeter security infrastructure applications (e.g., firewalls, intrusion detection systems) that depend on accessing and viewing IP transport data payloads must be aware they will not be able to view that part of the IP packet and alternate mechanisms should be deployed.
- If VPN tunnels are used to encapsulate IPv4 within IPv6, or IPv6 within IPv4 as a transition method for deployment:
    - The tunnel endpoints between the VPN should be secured as the traffic transits the VPN.
    - When an encapsulated IPv6 packet enters or leaves the VPN and Intrusion Detection is required, it should be understood that the Intrusion Detection application or other network security method used to permit a packet on that network, has been ported to IPv6, as previously identified.
- Wireless network access from IPv6 nodes requires in-depth security analysis for implementation when stateless auto-configuration is used, in addition to current methods to secure IPv4 wireless networks.
- Seamless Mobility with IPv6 will need to support the required security as identified by the agency to permit secure access to the network whether across the internal network, or remotely from an external network.
- IPv6 on a network should not be turned on by default unless all network security infrastructures are implemented. (Note: Some products may have IPv6 enabled out-of-the-box.)

With the current upgrade of networks environments, many products have IPv6 capabilities already. As with any new capability new threats and vulnerabilities will arise as attackers devote more attention to IPv6. As such, careful planning and additional attention to operating in a dual environment will be needed to deal with potential new threats and must be addressed by the agencies accordingly. (IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006)

O. IPV6 STANDARDS AND PRODUCT EVOLUTION

IPv6 technology is still evolving and this evolution is likely to continue through the DoD transition period. This is as expected and is a normal evolution of the Internet standards. While the base set of IPv6 protocols are stable and mature, and product implementations are emerging, many of the standards supporting value-added IPv6 features are still evolving. Many key IPv6 enabling protocols, especially for tactical wireless, security, QOS, and transition mechanisms, are still in development and will not be completed at the current effort levels for the 2008 fielding. The requirements for interoperability for IPv6 are from the DoD IT Standards Registry (DISR) IPv6 Standard Profiles for IPv6 Capable Products. The Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) has developed the (Department of Defense Internet Protocol Version 6 Generic Test Plan Version 2 dated September 2006) which describes the test and certification process for Commercial of The Shelve (COTS). Products certified are placed on an Approved Products List (APL) as IPv6 capable. The APL can be found at: http://jitc.fhu.disa.mil/adv_ip/register/register.html

P. TESTING AND CERTIFICATION ISSUES

Before any system deploys IPv6 it is important to test IPv6 within its network. In some cases cross-agency collaboration for IPv6 testing of implementations will reduce efforts, but each agency will need to identify their specific network testing requirements. In addition, agencies can work with industry to test their network access and some of the IPv6 features that require wide-area-network testing. The DoD certification process may pose a risk to the IPv6 transition schedule because of the newness of IPv6. The testing process itself may not be mature when it is needed. The certification may not be consistent with PM product selection practically if there is extensive use of COTS.

The DoD has established criteria for Testing and Evaluation (T&E) strategies and processes and methodologies in order to gauge the progress being made towards the transition. They are set forth in (Department of Defense Internet Protocol Version 6 Generic Test Plan Version 2 dated September 2006) which can be found at https://gesportal.dod.mil/sites/JITCIPv6/TEWG . Each Fiscal Year (FY) the DoD compiles a T&E report detailing the progress made to date. The report gives the overall

status of DoD IPv6 T&E in support of the DoD's transition to IPv6 and summarizes IPv6 T&E results reported by all DoD Components. Nineteen T&E reports were analyzed for the FY06 reporting period. The report for FY06 titled: (The Fiscal Year 2006 Department of Defense Internet Protocol Version 6 Test and Evaluation Report dated September 2006). The report compiles the results of the 19 separate test reports. The Joint Staff IPv6 10 Operational criteria and progress made to date follows.

Criterion 1: Demonstrate security of unclassified network operations, classified network operations, black backbone operations, integration of HAIPE, integration of IPSec, and integration with firewalls and intrusion detection systems**.**

- The IPv6 extension headers for IPSec have been successfully loaded with Public Key Infrastructure (PKI) certificates and secure end-to-end communications have been demonstrated.
- Security functions of routers (vulnerability scanning, support of SSH, secure management, password protection, and product integrity) have been successfully tested on routers selected for implementation.
- Access Control Lists for IPv6 routers and firewalls have been successfully demonstrated.
- No testing of HAIPE devices was performed. The National Security Agency (NSA) has developed technical specifications for HAIPE (version 3). Technical analysis of the specifications was performed and recommendations were provided to NSA. HAIPE T&E by NSA requires the delivery of version 3 prototypes.
- IPv6 packet inspection by firewalls has not been demonstrated. T&E will occur when firewall vendors produce IPv6 capable products.
- IDS have not been tested. T&E will occur when IDS vendors produce IPv6 capable products.
- IA certification and accreditation of IPv6 products and systems have not been accomplished.

Criterion 2: Demonstrate end-to-end interoperability in a mixed IPv4 and IPv6 environment.

- Numerous tests were performed that analyzed the performance and interoperability of IPv6 implementations in hosts and routers. The results of the tests varied, depending on the router and its operating system. Newer routers and operating systems support the basic IPv6 features but require further development to satisfy DoD IPv6 capable requirements.

- The following features were successfully demonstrated in a mixed IPv4 and IPv6 environment:
    - Stateless auto configuration
    - IPv6 routing protocols [Open Shortest Path First version 3 (OSPFv3) and Border Gateway Protocol 4+(BGP4+)]
    - Internet control messages [Internet Control Message Protocol version 6 (ICMPv6)]
    - Common network applications (HTTP, SMTP, and FTP)
    - Network services [DNS/Berkeley Internet Name Domain 9 (BIND 9) and Network Time Protocol (NTP)].
- IPv6 mobility and multicasting features experienced problems in the beta version of the operating system tested.
- Interoperability of IPv4 and IPv6 applications in mixed environments was demonstrated. The performance of the applications was on par with IPv4 only networks compared with IPv4 and IPv6 mixed environments.

Criterion 3: Demonstrate equivalent to, or better performance than IPv4 based networks.

- Several high-end Layer 3 Ethernet switches and some routers deliver IPv4 and IPv6 performance parity. Software implementations of IPv6 Layer 3 Ethernet switches demonstrate lower performance when using IPv6 than when using IPv4.
- The lack of IPv6 capable satellite IP modems and accelerators prevents deployment in a manner equivalent to IPv4. Overall, the current state of IPv6 used in tactical networks is immature and needs additional development and T&E before performance comparisons can be made with IPv4.
- Bandwidth constrained IPv6 links, with bandwidths higher than 16 Kbps, demonstrate parity with IPv4.

Criterion 4: Demonstrate voice, data, and video integration.

- Limited testing of voice, data, and video integration was performed using a voice/video emulation test tool with routers from a single vendor. The routers operated properly in interpreting the IPv6 DiffServ code points and provided the required quality of service.
- Further development and T&E is required to adequately demonstrate integration of voice, data, and video on IPv6 networks.

Criterion 5: Demonstrate effective operation in low-bandwidth environment.

- Test results for low-bandwidth environments were not conclusive. Conclusions drawn from two test reports were contradictory and indicate further testing is needed.
- Bandwidth constrained links with bandwidths higher than 16 Kbps are not negatively affected using native IPv6 in comparison to IPv4 over the same network. For bit rates below 16 Kbps, IPv6 throughput was much lower than IPv4.
- Use of dual stack techniques appeared to degrade performance on links below 2 Mbps. IPv6 parity with IPv4 was demonstrated using dual stack techniques with links above 2 Mbps.

Criterion 6: Demonstrate scalability of IPv6 networks.

- No scalability analysis of IPv6 networks has been performed, as there is currently insufficient data to populate network models and simulations.

Criterion 7: Demonstrate support for mobile terminals (voice, data, and video).

- Limited mobility testing was conducted this reporting period and attempts to use IPv6 mobility were unsuccessful. Immature vendor implementations are a serious and systemic problem in fielding MIPv6, NEMO, and MANET.

Criterion 8: Demonstrate transition techniques (details explained in subsequent sections).

- Five transition mechanisms are recommended: dual stack (within host OS and network devices), manual configured tunnel, automatic tunneling, Application Layer Gateway (ALG), and Stateless IP/ICMP Translation (SIIT).
- Dual stack transition techniques appear to create the most flexible strategy to allow coexistence of IPv4 and IPv6 applications.

Criterion 9: Demonstrate ability to provide network management of networks.

- Testing shows that IPv6 network management tools have been implemented to a limited extent. More development of IPv6 network management tools and T&E is required to demonstrate this criterion.
- The Government Off The Shelf (GOTS) network management tool C2RMS, as modified by the Air Force, resulted in important lessons learned in transitioning applications to IPv6.
- Of the routers and switches tested, the majority did not support the SNMPv3 Management Information Base (MIB).

Criterion 10: Demonstrate tactical deployability and ad hoc networking so systems can operate wirelessly.

- Simplified Multicast Forwarding (SMF) T&E indicates further development is required to support MANET multicasting.
- The WIN-T prototype nodes demonstrated IPv6 connectivity on the move and at the halt.
- Significantly more work remains for T&E of the tactical deployability and ad hoc networking capabilities of IPv6. (The Fiscal Year 2006 Department of Defense Internet Protocol Version 6 Test and Evaluation Report dated September 2006)

Q. WHAT ARE THE TRANSITION MECHANISMS AND STRATEGIES REGARDING IPV6?

Over the next several years the DoD has mandated that all networks and the global Internet transition to IPv6. This transition has been planned on an incremental basis and, therefore, there will be a period where IPv4 and IPv6 traffic must co-exist. The strategies PMs must utilize must take into account systems that must operate and support IPv4/IPv6 interoperability over the lifecycle of their systems. Further, PMs must follow all applicable guidance authorities including DoD level and Army level.

R. IPV4 AND IPV6 CO-EXISTENCE

Interoperability between IPv4 and IPv6 can be achieved using one or a combination of the following transition mechanisms: dual stack, tunneling, and translation. Interoperability needs to be maintained not only among the PM Systems, but also with all DoD Systems that interact with those systems and with the GIG, joint and multinational forces, and other connecting networks. The biggest challenge will be to maintain interoperability during the transition period. Interoperability between IPv4 and IPv6 hosts with different functional protocols will be a challenge. During the transition period there may be a difference in performance between IPv4 sessions and IPv6 sessions.

S. TRANSITION ANALYSIS

Areas that need to be considered include multicast, addressing architecture, DNS and Dynamic Host Configuration Protocol (DHCP) architecture, IA, applications, and QoS. The other area that should be assessed is the transition scenarios. The goal of the transition analysis is to provide recommendations that are best suited and based upon

each system's capability, logistics and schedule. Technology maturity of transition mechanisms and maturity of IP devices on each system should be considered. The key parameters to the trade space are when the systems transition during its lifecycle and to what the system transitions.

1. Pre-Deployment Transition

For pre-deployment transition, the baseline design changes from an IPv4-capable to an IPv6-capable system during the design phase. The focus of the pre-deployment transition analysis should center on the ramifications of transition mechanism technology and network architecture options including: dual stacks, tunneling, and translation.

2. Dual Stack

The term "dual stack" refers to TCP/IP capable devices providing support for both IPv4 and IPv6. Dual stack allows a device to communicate over both IPv4 and IPv6 but does not necessarily mean all applications operating within this device are capable of utilizing both IPv4 and IPv6. The term "dual stack routing" refers to a network that is dual IP, that is to say all routers must be able to route both IPv4 and IPv6. Requiring all new devices be both IPv4 and IPv6 capable permits these devices to have the ability to use either IP protocol version, depending on the services available, the network availability, service, and the administrative policy. A transition scenario which calls for "dual stack everywhere" provides the most flexible operational environment. Dual stacked hosts running on a dual stack network allow applications to migrate one at a time from IPv4 transport to IPv6 transport. Legacy applications and devices that are not yet upgraded to support access to the IPv6 stack can coexist with upgraded IPv6 applications on the same network system.

(IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006)

3. Tunnels

"Tunneling" is a means to encapsulate one version of IP in another so the packets can be sent over a router that does not support the encapsulated IP version. When two isolated IPv6 networks need to communicate over an IPv4 network, dual stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the

IPv4 network infrastructure that exists between the networks. (IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006)

4. Translation

The term "translators" refers to devices capable of translating traffic from IPv4 to IPv6 or vice and versa. This mechanism is intended to eliminate the need for dual stack network operation by translating traffic from IPv4-only devices to operate within an IPv6 infrastructure. This option is recommended only as a last resort because translation interferes with objective of end-to-end transparency in network communications. Use of protocol translators cause problems with Network Address Translation (NAT) and highly constrain the use of IP-addressing. (IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006)

T. POST-DEPLOYMENT TRANSITION

For a post-deployment transition, the trade analysis should cover the programmatic approach to the transition (retrofit vs. technology refresh) during the systems lifecycle, after an IPv4-only system has been deployed. Two transition scenarios should be considered for the post-deployment phase in the system lifecycle: retrofit and technology refresh.

1. Retrofit

A retrofit transition requires an upgrade of IP devices and related software after initial deployment of an IPv4-only architecture. This transition scenario assumes the devices to be replaced are still in good working order, but lack IPv6 capability, therefore, retrofit is performed. A retrofit transition may occur at any time in the system's lifecycle after initial deployment, but prior to a scheduled technology refresh. The primary benefit of a retrofit transition is it relaxes the transition schedule and allows each system to transition on its own schedule, tailored to individual program maturity and funding. The major disadvantage of this strategy is it is costly. A retrofit replaces hardware and software that is in good working order (other than not being IPv6 capable).

2. Technology Refresh

A technology refresh transition is defined as the periodic replacement of system components (in this case IP devices and associated software) to assure continued supportability throughout the system's lifecycle. This transition occurs during the natural

technology refresh cycle, based upon anticipated wear-out or obsolescence of devices. The timing of this transition is assumed to occur as far into the future as possible; however some devices would transition earlier than others, depending upon individual tech refresh schedules. The major advantage of transitioning during a technology refresh is it assumes the cost of the hardware and software is included in the technology refresh budget. Also, an overall cost savings can be assumed, because this late-in-the-lifecycle transition leverages the cost of future devices which are typically less expensive. However, there are many disadvantages to this as a program-wide transition scenario. The primary issue is government and military technology refresh cycles can be up to 25 years. This may be too far in the future to be acceptable. Another issue involves interoperability risk associated with the management of a technology refresh and its role in the IPv6 transition. Technology refresh programs such as capability enhancement or obsolescence management are typically performed as separate activities, and are therefore often disjointed. Also, it is unclear whether a transition to IPv6 is considered an "upgrade". Some DoD programs may define technology refresh in a way that excludes any cost and planning associated with "upgrades"; therefore it may be inappropriate to expect the cost and planning to be incurred in a technology refresh. This matter needs to be clarified with the Army.

U. GUIDANCE AUTHORITIES

The overall guidance authorities are categorized as DoD level, Army level, and PM level. The scope of authority, certification process, and waiver process is described for each guidance authority.

- DoD Level IPv6 Transition Guidance Authority

1. ASD(NII)/DoD CIO

The Assistant Secretary of Defense Networks and Information Integration, Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) is the top level authority for DoD Information Technology Systems. The ADS(NII)/DoD CIO grants all DoD IPv6 authority. The ASD(NII)/DoD CIO has the final authority in approving all DoD IPv6 Guidance documentation.

2. DoD IPv6 Mandate

ASD(NII)/DoD CIO issued a policy memo on June 9, 2003 that directed all DoD departments and agencies to begin the transition to enterprise-wide deployment of IPv6 for the GIG and all networks. A subsequent memo on September 29, 2003 provided additional guidance on three points: 1) What is IPv6 Capable 2) Standards Profile 3) Provisional Waiver Process. The June 9, 2003 "IPv6 Mandate" memo can be found at: http://www.dod.mil/nii/org/cio/doc/IPV6.pdf

3. DoD IPv6 Transition Plan

The Office of ASD(NII)/DoD CIO has written the DoD IPv6 Transition Plan. The DoD IPv6 Transition Plan describes the overall strategy for IPv6 transition, identifies roles and responsibilities, and establishes implementation governance. Additionally, the plan contains guidance on: obtaining IPv6 capable products; testing and demonstrations; responsibilities and considerations for transitioning networks, applications, and infrastructure; the criteria for demonstrating transition readiness; and the strategy for leveraging ongoing commercial IPv6 work.

4. DoD IPv6 Master Test Plan

The Office of ASD(NII)/DoD CIO has written the DoD IPv6 Master Test Plan. The DoD IPv6 Master Test Plan defines the overall IPv6 Test and Evaluation (T&E) strategy, identifies the organizations responsible for carrying out the strategy, and identifies the challenges that may impede IPv6 implementation. The DoD IPv6 Master Test Plan establishes a reporting process that promotes information sharing of test plans and results across the DoD.

5. Certification

ASD(NII)/DoD CIO has the final authority to certify a system is IPv6 Capable. For this certification to be granted, the system must complete the Joint Interoperability Test Command (JITC) interoperability certification. JITC certification will require a system to support the Defense Information Technology Standards Registry (DISR) profile standards that is applicable to the required functionality of a system. ASD(NII)/DoD CIO will work through component organizations (Army) to grant certification. The Army has identified the Army System Engineering Office (ASEO) as having the responsibility to process and evaluate IPv6-capable certification and submit

recommendations to the CIO/G-6. The CIO/G-6 will directly support the DoD IPv6 Transition Office and will represent the Army. The CIO/G-6 will make recommendations to the ASD(NII)/DoD CIO.

6. Waiver Process

Where it does not appear feasible to transition as mandated, a waiver in accordance with the process discussed in the DoD IPv6 Transition Plan is required. This may be due to a procurement or development in which the requirements cannot be complied, or legacy systems which are not expected to remain in service beyond five years. Component CIOs can waive the IPv6 requirement based on the above criteria. Component CIOs may not re-delegate this waiver authority. The ASD(NII)/DoD CIO must be notified of any waivers granted and provided with the rationale ten days prior to the effective date of the waiver for final approval purposes. Any procurement waivers granted should generally be for one year or less, given the expected increased availability of IPv6 capable products. The ASD(NII)/DoD CIO is the final approval authority for any IPv6 procurement /transition waiver decisions. In addition, the ASD (NII)/DoD CIO will coordinate with Component Acquisition Executives and Program Executive Offices (PEOs) on any joint, defense-wide or Intelligence Community (IC) programmatic IPv6 issues. The Department of the Army has identified ASEO as having the responsibility to process and evaluate IPv6 waivers and submit recommendations to the CIO/G-6. The CIO/G-6 will directly support the DoD IPv6 Transition Office and will represent the Army in coordinating activities among the DoD, the joint services, allies, and coalition forces.

7. Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is granted authority from ASD(NII)/DoD. DISA is responsible for the operation of large components of the DoD GIG. DISA responsibilities include:

- Coordinating DoD's IPv6 standards efforts including working with industry, IETF, ITU, IEEE, and other standards bodies to ensure DoD needs are reflected in evolving IPv6 standardization efforts
- Acquiring, allocating and managing IPv6 address space for the DoD
- Providing top-level IPv6 Domain Name System (DNS) support for the DoD, including Internet root server(s)

- Interoperability testing and certification for IPv6 products and capabilities
- Ensuring end-to-end IA issues associated with Defense Information System Network (DISN) transition to IPv6 are resolved

DISA has established a DoD IPv6 Transition Office (DITO) that provides the overall technical coordination, engineering, guidance and assistance across DoD, which is needed to support an integrated and coherent transition. This office is responsible for providing common engineering solutions and guidelines designed from an enterprise perspective. It is responsible for coordinating transition planning, analysis, testing, and implementation efforts across DoD. Additionally, it is responsible for implementing a systematic program of outreach with the DoD community, promoting knowledge sharing, and ensuring needed infrastructure is provided. It will ensure critical transition issues are prioritized and addressed.

8. Defense IT Standards Registry

DISR maintains the official DISA set of DoD Standards Profiles. These DISR standards profiles are used to develop the definition of "IPv6 Capable." "*IPv6 Capable*" shall mean "a device must pass the IPv6 core requirements, support transition mechanisms to be interoperable with IPv4, support the IPv6 security profile, support at least one (or more) IPv6 capable connection technologies, support requirements for one (or more) functional categories: host, router/switch, security device, network server; and support the IPv6 version of any other requirements necessary for its function on the GIG, and is verified by test or demonstration in the laboratory." DISR standards for all networking technologies are contained on the DISROnline web site at http://disronline.disa.mil. A DISROnline account is required to view this site. The Mandated DISR IPv6 Capable Profiles are found at: https://disronline.disa.mil/a/DISR/view_kip_family.jsp?spId=807.

The Emerging DISR IPv6 Capable Profiles can be found at: https://disronline.disa.mil/a/DISR/view_kip_family.jsp?spId=807.

9. IPv6 Capable Certification Process

IPv6 Capable certification will come through a process of tailoring the DISR IPv6 Capable profile to the specific functional requirements of the system under consideration.

After applicable IPv6 Capable DISR standards are identified, the program will develop an applicable product implementation.. After full JITC approval, a product will be considered IPv6 Capable.

10. DISA Joint Interoperability Test Command

JITC is an independent operational and test evaluation assessor of DISA. JITC provides joint and combined interoperability testing, evaluation, and certification for C4I systems. JITC will perform IPv6 performance and load testing, routing interoperability tests. JITC will also perform IPv6 application and transition mechanism testing and evaluate end-to-end interoperability in mixed IPv4/IPv6 environments. JITC will develop and maintain an IPv6 vendor and DoD equipment, software, hardware and applications interoperability matrix and an IPv6 capable APL. JITC will also participate in DoD IPv6 working group meetings.

11. National Security Agency

The National Security Agency (NSA) is a component of the DoD under the command of the Joint Chiefs of Staff. The NSA protects US Government information systems. The NSA has the authority to require information assurance certification and accreditation of DoD information systems. The NSA is developing, in conjunction with the appropriate Components, a set of IA guidelines and solutions for implementing IPv6 within the department. Of particular urgency is the need for IA guidelines in support of early IPv6 pilots. In addition, NSA has developed version 3 of the HAIPE specification, which is IPv6 capable. HAIPE functionality and performance characteristics are being developed in conjunction with the Components and will support DoD's transition objectives. The NSA will work closely with DISA and the Services in the development of an IPv6 network and IA design with the goal of ensuring a timely, secure and operationally effective IPv6 environment. In addition, the NSA will ensure that the GIG end-to-end IA architecture, which is in development, addresses IPv6 as an integral component. The NSA GIG Architecture Group is the mechanism for resolving these issues.

- Army Level IPv6 Transition Guidance Authority

12. Army IPv6 Mandate

On Nov 5, 2003, the Army CIO/G-6 issued a memo that mandates the Army will transition to IPv6. Another Army memo providing further IPv6 guidance was issued on April 1, 2004.

13. Army Transition Management Structure

The Army has established an IPv6 Transition Plan Working Group (ITPWG) to serve as the umbrella organization to regulate and control the governance, development, implementation, and management of the transition within the Army. The ITPWG is co-chaired by the Army Chief Information Officer, Deputy Chief of Staff (CIO/G-6); the Assistant Secretary of the Army (Acquisition, Logistics, and Technology), (ASA(ALT)); and the Network Enterprise Technology Command (NETCOM). The ITPWG reports to the CIO Executive Board. The ITPWG works through DISA and with ASEO to influence the DoD certification processes and IETF standards development.

IV. STEPS PROGRAMS MANAGERS MUST TAKE TO TRANSITION PROGRAM OF RECORD (POR) SYSTEMS FROM IPV4 TO IPV6

A. ALLOCATION OF ADDRESS SPACE?

The ability of the DoD to move into digital warfare establishes a competitive advantage over opposing threats. Giving commanders and warfighters the capability to communicate and share intelligence across the full spectrum of operations, will contribute to the aptitude for the United States Armed Forces remaining, the world's premier superpower well into the foreseeable future. This ongoing effort is the largest undertaking by the joint services to date and will require the coordination and ingenuity of thousands of people, organizations, and industry partners in order to succeed.

The technology of tomorrow will encompass an array of built-in sensors that will allow soldiers and commanders to monitor core body temperature, hydration levels, sleep status, and other critical physiological information.

B. ADDRESSING PLAN FOR THE DOD

The Office of the Secretary of Defense for Network and Information Infrastructure (OSD NII) directed the DoD to incorporate IPv6 and operate in a dual IPv4/IPv6 capacity. The direction to incorporate IPv6 and operate in a dual IP capacity for the foreseeable future is essential to the foundation of interoperability across the DoD. Operating in a dual mode will ensure that the cutover to IPv6 will not end the effectiveness of fielded systems supporting wartime efforts. Most of the systems in need of upgrade or replacement are procured from commercial vendors and DoD contractors. Upgrading systems also impacts routing and data distribution.

Top down organizations such as the DoD have problems because OSD establishes policy and dictates implementation to the services. Once the services receive direction and implement across the force, individual programs are left to design solutions. This top down approach seldom takes into account the sensibility from a system level. Systems such as the Joint Tactical Terminal (JTT) provide commanders targeting capability through the use of the Interactive Broadcast Service (IBS). The JTT has been directed to

be IPv6 compliant, yet the JTT will never need IPv6 to function. The host system into which the JTT is integrated must be IPv6 compliant, which makes the JTT IPv6 compliant. This confusion has caused the JTT program office to submit an IPv6 waiver, which consumed many man hours to produce and staff.

The DoD operates under a "top down" philosophy that has proven inefficient. The DoD should strive to incorporate a horizontal approach to establishing policy and decision making. Horizontal organizations develop cross functional teams to address and solve problems. Utilizing cross functional teams allows stakeholders at every level to provide input into the decision making process. This ensures that working level issues are discussed among subject matter experts before direction and policy is solidified. Horizontal organizations focus on external rather than internal results of decisions. Increasing coordination between each level within DoD will enhance morale, efficiency, and soldier support. The DoD is striving to incorporate the Integrated Product Team (IPT) at program levels. IPTs are cross functional teams designed to incorporate various elements of the acquisition process. This eliminates waste by ensuring every element of the acquisition process is addressed simultaneously. IPTs ensure functional disciplines within an organization are communicating and expressing concerns that impact a program. DoD has directed organizations at a lower level to incorporate these new acquisition principles and has not integrated them into their own processes.

The addressing plan the IPv6 Transition Office (DITO), Defense Information Systems Agency (DISA), and the representative Services (Army, Navy and the Air Force) agree on is feasible from a service standpoint. However, another option to consider when transitioning under the time phased approach is to convert the core networks to IPv6 and then convert the access level networks and application hosts to IPv6. This would require the DoD to develop an IPv6 Core as the basis for transition. The Core would include the DISN/GIG/BE (SIPRNET, NIPRNET, and JWICS). Once the core networks are established, IPv4 application traffic will be able to communicate on the IPv6 core. One of the benefits of this approach is avoiding many transition

mechanisms, which themselves introduce a great deal of complexity. The end result will occur when enough IPv6 applications generate a significant amount of traffic to enable the IPv4 traffic to discontinue.

C. NETWORKS

Having separate networks such as NIPRNET, SIPRNET, and JWICS, creates various challenges when dealing with IPv6 transition. Anyone who works on a top secret project and does not work in a SCIF will explain that having separate networks is a challenge. This is especially true when working with organizations that operate on SIPRNET daily. Workers often have to check SIPRENT email in a secure room that may be remotely located away from their office. Other problems arise when workers are unaware that an email marked as "SECRET" has been sent to their SIPRNET account. These emails may go unchecked for days until the worker is notified such information has been transmitted.

The separate networks that the DoD manages must be kept separate for security purposes. When IPv6 transition starts to disseminate across the various networks managing the separate classification levels will be challenging. Administrators will have to ensure that only networks operating at the same classification can connect to peers with IPv6 addresses. This issue also affects our Allied and Coalition networks, which need to be segregated from operational DoD networks of similar classification.

D. DOD NETWORK INFORMATION CENTER IPV6 ADDRESS MANAGEMENT

The DoD is a hierarchical structure in which every entity in the organization, except one, is subordinate to a single other entity. Structuring organizations this way can decrease communication by limiting information flow. Problems erupt when the communication between hierarchical organizations gets distorted by the time it reaches the end of the line. This form of distortion is often referred to as telephoning, where information is transferred from a sender to a receiver and is distorted each time the information is transferred.

Allowing the MIL NIC, Service NICs, and Agency NICs to allocate address space in a hierarchical manner increases IPv6 transition efficiency. When agencies apply for

address space they will be required to demonstrate a valid need. These requests will be elevated to the next level in the hierarchical structure. Once that level gathers the total requirement it will request one total amount of space to the next level. Operating the request process in this fashion will increase the understanding that each NIC has on their requirements.

A successful transition requires utilizing administration practices that are successful under current Ipv4 practices. Allowing DoD NICs to continue the maintenance of DNS servers, zone files, and delegate subordinate zones for their respective forward DNS zones maintains consistent configuration control over processes already in place.

E. ESTIMATING COST TO TRANSITION POR SYSTEMS FROM IPV4 TO IPV6

The Department of Defense has established a goal that all GIG IT assets are to transition from the current IPv4 to the newly developing IPv6 by FY08. The current DoD transition estimate makes some overriding assumption and extends the transition period until FY16, which reduces the transition cost by approximately 50% or $1.6B (Director, Technical Architecture Division Architecture Operations Network & Space CIO/G-6). The assumption was made to reduce the cost to the DoD on the intent for transition to be implemented with Technology Refresh whenever feasible.

F. OVERALL DOD ESTIMATE TO MEET MANDATE

The guidance to transition legacy systems using Technology Refresh or Software Block upgrade programs and pre-deployment systems designed to IPv4/IPv6 capability system during the development phase provide the DoD with the frame work to estimate the overall cost. The major cost drivers for implementing the pre-deployment transition include:

- Increased System Memory to Handle IPv6 and Dual stack Mechanism
- Increased System Processor Overhead to Handle IPv6 and Dual stack Mechanism
- Certifications
- Increase in Required Bandwidth to Handle IPv6 and Dual stack Mechanism

- Additional Dual stack Software
- Interoperability testing

The cost can be estimated using standard software and hardware estimating models such as Constructive Cost Model COCOMO for software development based on the above drivers. The hardware estimates are not viewed as the major cost driver due to the pace with which commercial industry is providing greater capability at reduced cost. The assumption that Moore's Law (stating transistor density of integrated circuits, with respect to minimum component cost, doubles every 24 months) will continue to hold true in the future is relatively conservative given the industry's past performance The cost will, in large part, be driven by maturity of the design for the system in question. For systems that have yet to reach Preliminary Design Review (PDR), the design changes to support IPv6 will be much easier. For systems that have reached or passed Critical Design Review (CDR), rework required will be far greater. The insertion of previously approved software and hardware products from the JITC APL, whenever possible, can alleviate much of its additional cost. The government could work with their respective contractors in order to estimate the cost of the transition. The government must also generate an Independent Cost Estimate (ICE) in order to gain a full appreciation for the additional funding required. The government must also take into account the additional interoperability and certification testing required for the transition.

Transition guidance for legacy systems using Technology Refresh or Software Block upgrade programs must be implemented carefully. The fact that tactical networks are inherently low-bandwidth requires detailed modeling and simulation and laboratory testing before these systems can be upgraded to support IPv6. The effects on tactical network operations and the performance of these systems must be understood before any transition decision is made. Systems with sufficient throughput should transition using their normal technology refresh/software upgrade schedules. The additional cost to transition to IPv6 can be determined using the methodology outlined above. Those systems, determined unable to support transition should be maintained in an IPv4

capacity only. If these systems are not planned for obsolescence within the mandated five year window, then the waiver process must be followed and replacement systems identified for future upgrades.

G. ARMY PROGRAM EXECUTIVE OFFICES (PEO) ASSUMPTIONS FOR TRANSITION COST ESTIMATES

Transitioning programs of record to IPv6 is a monumental task that will require significant resource commitments. For this reason, the Army needs to take account of all input gathered from the PEOs before allocating resources. When the Army makes decisions and sets direction before data can be analyzed, significant amounts of rework are required to meet the desired performance end-state.

The Army is preparing to use technology refresh funding to accomplish a significant portion of the transition to IPv6. This decision was made as a result of the "good enough drill", which eliminated the majority of funds that would have been used for technology refresh for the Battle Field Functional Areas (BFAs). To further complicate this scenario, Joint Command and Control (JC2) is slated to replace Command and Control (C2). JC2 has not provided any POM funding information for transition. Decisions such as this are made independently of the policy maker's knowledge and impact implementation. Presently, the JC2 BFA has no funding associated with its requirements to transition to IPv6.

H. BENEFIT TO THE DOD OF TRANSITION

1. Interoperability

In order to achieve true interoperability and seamless information sharing, the DoD must first embrace Net-centricity, rather than data movement. Data movement simply transports information to another location. Net-centricity empowers soldiers with the ability to discover, access, integrate, correlate and fuse information and data that support their mission objectives. Interoperability would only be one of many supporting attributes.

Achieving Net-centricity requires synergizing people, organizations, processes, information and materiel. Material should be dealt with last. The DoD needs to address

businesses-process redesign first, and then focus on the people, organization and information needed to support it. In the end, technology will only benefit organizations equipped to receive advanced solutions.

The largest hurdles organizations will face when transiting to IPv6 are people, organization and processes. The people of an organization have the information. Attempting to retrieve the information will require a cultural change. Changing the way people access information from a need-to-know basis to a need-to-share environment is a challenge the DoD has yet to face.

2. Improved End-to-End Security

Preventing intrusion into a DoD network and improving end-to-end security are the most important aspects of IPv6 transition. More work needs to be done to increase the availability and quality of IDSs. To date, the only country that is proactive in promoting IDSs is Japan, which has recognized the need to develop IDSs and is taking steps to ensure IPv6 networks are protected from intrusion. Without adequate IDSs, DoD networks become vulnerable to intrusion, which can jeopardize both life and property. With little work being done on IPv6 IDSs, organizations will be playing catch-up afterwards, with increased potential for network compromise.

The other security features of IPv6 increase security but only if properly implemented and continually monitored. Without SEND, DoD networks will be left vulnerable to intrusion when accessing other databases. Prioritizing network traffic using QoS will enable time-critical information to reach the commander. Having the right information at the right time is essential to managing wartime efforts. Mobile IP and auto configuration are essential to the individual warfighter who will be utilizing information while on the move.

End-to-end IPSec is essential when implementing a Net-centric architecture because users are classified with various security clearance levels. Users requiring top secret information will be verified through IPSec for the required security credentials before being allowed to access that information. Controlling classified information in a

Net-centric environment allows all users regardless of security classification level to operate on the network and share information that is essential to the success of their mission.

Implementing the appropriate security controls associated with IPv6 is challenging and will require significant resources to manage. It is only when DoD can successfully implement required security provisions as well as connecting appropriate security classification levels will the vision of Net-centric warfare be achieved.

3. Ease System Management Burdens

Proliferation of wireless devices has increased the amount of IP addresses. Today there is more pressure than ever to keep networks flexible and available. Failure to automate networks with a robust and scalable management solution can increase management burdens and lead to serious complications.

Achieving seamless operation requires an inventory of address space that resides in a centralized database to ease management burdens. Address space is the fundamental entity that allows networks to communicate. Maintaining the accuracy and consistency of the address space will ensure continued network operation. Managing the centralized database requires updates when address space allocations are granted by the next higher authority. Failure to maintain accurate address space inventories will complicate network traffic and prevent users from accessing information. This potentially serious complication can lead to life threatening situations when commanders need to access time-critical information needed for decision-making.

Auto-configuration of nodes is essential from a mobile warfighting force perspective. Auto-configuration allows users to connect a device to a network with minimal configuration. This is essential when a user is traveling on the battlefield because the soldier will enter areas where the network may change. Auto-configuration allows the user to seamlessly access information in the new network. Without it, users would need to re-address their IP, which takes time and can jeopardize their safety or mission effectiveness.

4. Unlimited Address Availability

The reality of connecting every soldier via electronic communications on the battlefield is clearly a significant goal for the DoD. Fortunately, this challenge is achievable with IPv6. Enabling the soldier to communicate and share information across the full spectrum of operation will ensure the United States Armed Forces remains the world's superior fighting force.

I. ISSUES SURROUNDING DOD TRANSITION

DoD transition, which was originally mandated to be completed by FY08, has been extended to FY16 in order to minimize transition cost. It is important that planned and programmed systems be acquired with support for both IPv6 and IPv4. This must include ensuring the following:

- The requirements for all DoD developed products include both IPv6 and IPv4 support.
- Commercial products selected include both IPv6 and IPv4 support.
- Coexistence strategies must be developed to ensure interoperability with legacy systems until the transition is complete.

1. Maintaining Interoperability

The many legacy systems built on IPv4 pose several issues for migration to IPv6. The overall DoD mandate, to transition systems to IPv6 that are greater then five years from obsolescence (Department Of The Army Internet Protocol Version 6 (IPv6) Transition Plan (Phase 1)), has implications for both the products themselves as well as the system's architecture. For systems that contain commercial hardware or software, performing system upgrades to support both IPv6 and IPv4 will be relatively straightforward. Most commercial product vendors are currently supporting both protocol versions, or have plans to do so in the near future. Also, the commercial product vendors will be responsible for maintaining their products in response to changes in the IPv6 standards.

DoD systems that were developed solely for military application pose a far greater challenge. The acquisition cycles and product lifetimes for these systems are usually substantially longer than commercial technology cycles, particularly for tactical-level systems. Furthermore, the communications systems that comprise the tactical networks

have extremely low bandwidths (hundreds to thousands of bps) by commercial standards, and potentially very long delays (e.g., >0.25 seconds on SATCOM links). Because of these challenges, tactical systems are highly optimized in terms of network usage. For example, in the Army's Lower Tactical Internet, UDP/IP headers for situation awareness (SA) traffic are not transmitted over-the-air and TCP is rarely used because of its overhead. (Implementer Ipv6 Transition Plan For Program Executive Office Command, Control, and Communications Tactical (PEO C3T) dated 24 May 2004)

A potential concern with IPv6 is the header size, which is twice as large as the IPv4 header or 20 bytes. This could impact performance although header compression schemes can mitigate this impact, careful testing in a realistic environment is needed prior to deployment since IPv6 header compression is immature. The issue of optional extension headers used by IPv6, will further decrease bandwidth efficiency. The resulting bandwidth requirement increase may make transition impractical for some tactical handheld, man packed, and vehicle mounted systems. This may, in turn, have cascading effects on other tactical networks, applications, and supported systems. Simultaneous dual stack operation may be impractical from a tactical battlefield management issue. This could significantly impact transition strategy, cost, and risk.

The assumption that legacy systems will be obsolete in five years or less entails high risk. The systems that are currently in development and slated to replace legacy system are more often than not, delayed in development due to factors such as technical challenges, funding shortfalls, cost overruns, and schedule delays. It is projected that the legacy systems will be required far longer then the projected five year time frame. The assumption that the Army will obtain IPV6 Upgrade through FCS, WIN-T, and JTRS implies total replacement of existing systems. This may not be supportable in practice and is unlikely to happen in the foreseeable future. The current systems will be in the field for the foreseeable future. Current Force and Future Force systems will have to be interoperable. All new systems fielded will be required to support both IPv4 and IPv6 protocols for the foreseeable future.

New systems may obtain dual IPv6 and IPv4 capability with the use of commercial products. In cases where commercial products are not available, custom

develop IPv6/IPv4 capability must be implemented. These cases are of particular concerns in the near term because IPv6 standards and IPv4-IPv6 transition mechanisms are not fully mature. Developments started before standards mature run the risk of incurring increased maintenance costs to keep pace with changes in IPv6 standards. To mitigate this risk, DoD-unique developments must be implemented in a way to facilitate changes to the IP protocol as it matures with strong layered architecture that separates out the network/IP layer.

J. SECURITY ISSUES

Many of the threats to today's IPv4 network security will not disappear with the deployment of IPv6. This includes vulnerabilities in higher layer protocols and services within the network. In addition, changes under the IPv6 protocol may yield new, as yet unknown, vulnerabilities.

Since IPSec will be available at the network layer, this could facilitate expanded use. Applications will not have to implement IPSec, but can merely make calls to the operating system socket layers to use IPSec. Since this feature will be available on all devices that implement the IPv6 protocol, host-to-host security associations can be easily defined with this base technology, an ability which does not exist with IPv4.

The DoD relies heavily on Type-1 encryptors on their networks. Historically, encryption has been provided either at the physical layer for encryption of point-to-point circuits (e.g., T1), or the link layer for ATM and Ethernet circuits. Increasingly, there is an emphasis on encryption technologies which operate at the IP layer. As DoD moves toward IPv6, these devices will need to be upgraded to support the new protocol. In the interim, tunneling architectures will have to be developed to support the use of IPv4 encryptors across IPv6 networks and vice-versa. The IPv4 encryptors may require software updates to implement tunneling.

K. IPV6 STANDARDS AND PRODUCT EVOLUTION

The IPv6 commercial base is well supported, proven interoperable, size deployed in the latest generation of routers and operating systems, and is being extended to applications and network management and security infrastructure. The initial goal for

IPv6 deployment in the DoD Global Information Grid (GIG) is to deploy and test the base protocols in a series of pilot exercises.

The Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) has developed the Department of Defense Internet Protocol Version 6 Generic Test Plan Version 2 dated September 2006, which describes the test and certification process for Commercial Off The Shelf (COTS) components. All products certified by this process are placed on an Approved Products List (APL) as IPv6 capable. The DoD IPv6 Approved Products List (APL) Process (see figure 2) can be found at the APL website: http://jitc.fhu.disa.mil/adv_ip/register/register.html. The current OSD mandate is that all DoD PMs purchase from the JITC APL first. If a candidate product is not on APL, the product can be nominated for APL testing and certification. Requirements derived from the DISR IPv6 for Capable Product Profile and can be found at https://www.aiptl.nit.disa.mil/documents. The above mandate makes it critical for PMs to constantly monitor the APL in order to determine the progress with IPv6 standards and ensure the COTS products that are being integrated are certified and on the APL. By doing this, the PM can reduce overall integration and test risk by utilizing COTS that has already been approved. (IPv6 Master Test Plan V. 2, Section 3, September 2006)

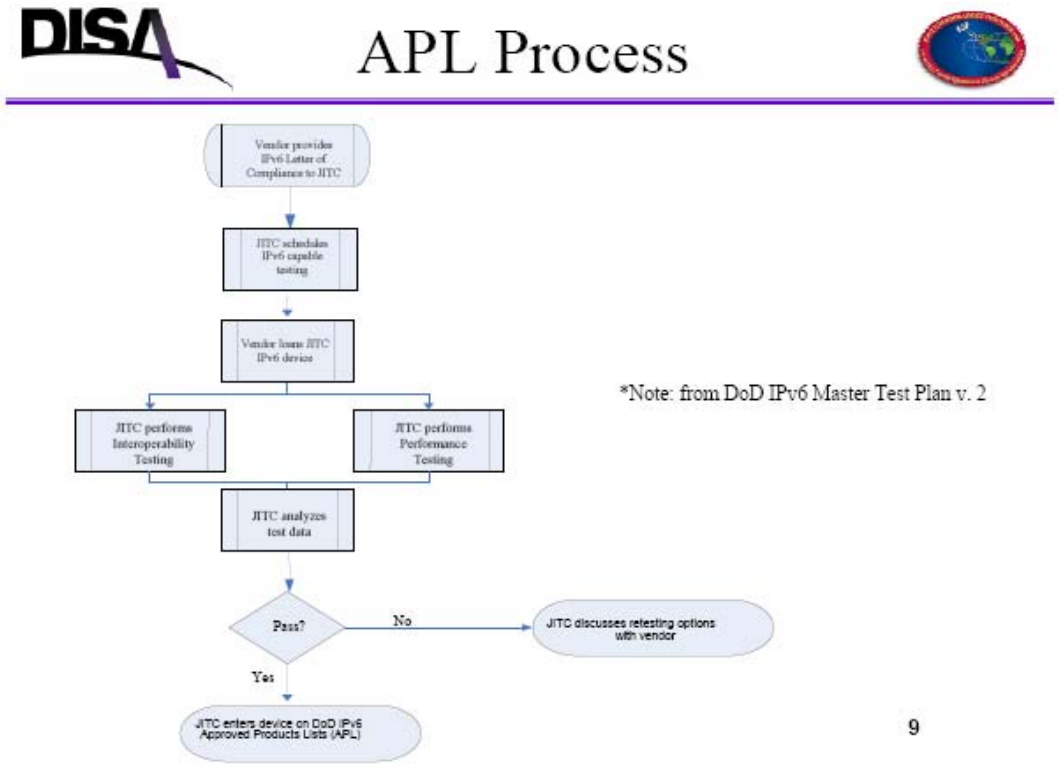

Figure 2. APL Process

L. TESTING AND CERTIFICATION ISSUES

Protocols and products, critical to the IPv6 transition for the DoD, are still under development. IPv6 capable commercial products, that meet DoD's performance, interoperability, and IA requirements, continues to be key to the transition. Pacing items for T&E and subsequent implementation of IPv6 across the DoD include High Assurance Internet Protocol Encryption (HAIPE) devices, network management systems, firewall appliances, intrusion detection/prevention systems, PKI implementation, and key distribution systems. T&E and operational deployment of IPv6 capabilities may be delayed until the critical equipment and devices are commercially available. (The Fiscal Year 2006 Department of Defense Internet Protocol Version 6 Test and Evaluation Report dated September 2006)

Since IPv4 and IPv6 devices are expected to co-exist for some time, thorough testing of interoperability, security, and performance is critical for a smooth transition to IPv6. Several issues need to be resolved before IPv6 is implemented in DoD networks. Areas requiring further emphasis are:

- Commercial development and T&E is required for IPSec and security devices such as firewalls, IDS, HAIPE, and other network security appliances. *(Criterion 1)*
- T&E is required to adequately demonstrate network and application interoperability in mixed IPv4 and IPv6 environments. *(Criterion 2)*
- Development and T&E is required for ASIC-based IPv6 routers and Layer 3 switches to adequately demonstrate IPv6 performance equivalent to, or better than, IPv4.
- *(Criterion 3)*
- Development and T&E of integrated IPv6 voice, data, and video products is required. The DoD must also agree on technical guidelines for integration of voice, data, and video. *(Criterion 4)*
- Development of ROHC and T&E for use within tactical environments is required. *(Criterion 5)*
- Development of data for network models and simulations, combined with T&E, is required to adequately demonstrate scalability. *(Criterion 6)*
- Development, implementation, and T&E of IPv6 mobility standards and features are required for mobile environments. *(Criterion 7)*
- Development and implementation of DSTM and application transition techniques are required. *(Criterion 8)*
- Development and T&E of IPv6 capable network management tools and systems are required. *(Criterion 9)*
- Development, vendor implementation, and T&E of MIPv6, NEMO, and MANET are required. *(Criterion 10)*

(The Fiscal Year 2006 Department of Defense Internet Protocol Version 6 Test and Evaluation Report dated September 2006)

M. RECOMMENDED DOD TRANSITION MECHANISMS AND STRATEGIES REGARDING IPV6

Due to the fact that the transition has been planned on an incremental basis there will be a significant period where IPv4 and IPv6 traffic must coexist. Legacy systems will likely be operational longer then anticipated because objective systems currently in development are often delayed. In most circumstances the legacy system will be utilized

in the field far longer then the projected five year time frame. PMs must incorporate acquisition strategies so systems can operate and support IPv4/IPv6 interoperability throughout the systems lifecycle. Also, PMs must follow all applicable guidance authorities including DoD level and Army level.

N. TRANSITION TRADE ANALYSIS CONSIDERATIONS

The purpose of the IPv6 trade analysis is to assess transition scenarios and provide recommendations based upon each system's capability, logistics and schedule. Technology maturity of transition mechanisms and maturity of IP devices on each system should be considered. The key parameters of the trade space are when the system transitions during its lifecycle and to what the system transitions.

1. Pre-Deployment Transition

For pre-deployment transition, the baseline design must be changed from an IPv4-capable to an IPv4/IPv6-capable system during the design phase. The focus of the pre-deployment transition analysis should center on the ramifications of transition mechanism technology and network architecture options including dual stacks, tunneling, and translation.

2. Dual Stack

The preferred method for DoD and commercial Internet networks is to deploy dual stack systems. The benefit of dual stack is network design simplicity, but it requires extra software, memory and processing power within every device. IPv6 is less bandwidth efficient than IPv4 due to larger header size and optional header extensions. Futhermore, there are IPv6 options specifying "jumbograms" (extra large packets for high speed bandwidth efficiency) that are not feasible over tactical links. Additionally, the optimum size for Minimum Transmission Unit (MTU), fragmented packets, must be determined by detailed analysis and testing.

The fact that tactical networks are inherently low-bandwidth further complicates implementation. Given these complexities, IPv4 may continue to be used for several years on low-speed links where the bandwidth inefficiencies would result in an unacceptable impact on performance. Additionally, most tactical systems will probably need to migrate to an IPv6 only network all at once, due to the fact that the transition

mechanisms within IPv4/IPv6 networks are far to bandwidth inefficient to operate over lower echelon networks. In future, JTRS may provide sufficient bandwidth to support a transition to IPv6 on lower echelon networks, however from a programmatic perspective, lower echelon systems are fairly homogeneous and tend to be fielded in blocks. Accelerating replacement schedules once JTRS is available would be technically feasible, but will require major increases in program funding due to the significant numbers of end systems that would have to be procured.

3. Tunneling

Some of the major issues for IPv6 tunnels are that some require manual configuration. Various proprietary implementations schemes exist, but they tend to embed the details of IPv4 routing creating routing inefficiencies, which leads to IPv4 fragmentations causing extra network traffic. Since it uses IPv4 routing not improved IPv6 routing, it cannot traverse IPv4 NAT and must be deployed with a tunnel broker service to automate setup and take down. Tunnel brokers may cause 20 or more packets to establish a tunnel. Configured tunnels may not be effective in tactical networks due to manual intervention, performance, and security.

The IPv6 header is twice the size of the IPv4 header. Optional IPv6 header extensions would also increase header length. If in addition, IPv6 packets (from applications) are tunneled through IPv4, we can expect that network performance will be degraded over bandwidth constrained links, and links with long latencies, such as SATCOM. High Bit Error Rates (BER) exacerbates the problem, since packets that are lost must be retransmitted, increasing packet reassembly delay. This would be especially true for small packets (e.g., VoIP) caught behind larger packets in the router's queue**.**

4. Translation

Each translation mechanism has its own advantages and disadvantages with respect to performance, security, operational efficiency, and scalability. However, each method requires either extra software within a host or an external device to provide this capability. Translation has high system overhead, limited manageability, is focused on a single host or single communications path, may have security limitations, and is a high-cost alternative. Therefore, translation may not represent a viable alternative.

O. RECOMMENDED PRE-DEPLOYMENT TRANSITION MECHANISMS

Dual stack is the preferred mechanism because of its scalability and minimal impact on performance. It also meets current tactical network criteria for configuration, manageability, reliability, scalability and security. Dual stack has the additional benefit of requiring less bandwidth since it requires minimal connection setup.

When some portions of the tactical network do not support both IPv4 and IPv6, tunneling or translation may be required. The preferred method in this instance would be tunneling due to the fact that translation requires either extra software within a host or an external device driving implementation cost. The extra burden on bandwidth and long latencies must be considered when implementing tunneling transition mechanisms.

P. POST-DEPLOYMENT TRANSITION

The DoD will implement transition with Technology Refresh whenever feasible. PMs should therefore plan for transition using Technology Refresh or Software Block upgrade programs. The assumption the Army will obtain IPV6 Upgrade through FCS, WIN-T, and JTRS entails total replacement of existing systems. This has some issues, may not be supportable in reality and is unlikely to happen in the foreseeable future. The current force systems will be in the field for the foreseeable future. Current Force and Future Force systems will have to be interoperable. Furthermore, given the fact that tactical networks are inherently low-bandwidth and IPv6 requires more overhead may dictate field systems remain IPv4 only for the foreseeable future. The one major issue with this approach is adequate IPv4 address space to accommodate the dual stack environment.

Given the fact that many tactical systems will remain IPv4-only for a long time the implementation of a dual stack core and gradual implementation of dual stack IPv4/IPv6 devices and applications is the recommended approach. These devices and applications would attempt to "favor" IPv6, but have the ability to fall back on IPv4 as a secondary method. Traffic would be carried end-to-end as either IPv6 or IPv4 whenever practical. This approach could potentially avoid the use of many transition mechanisms, which themselves introduce a great deal of complexity. Additionally, many of the IPv6 transition mechanisms introduce single points of failure which could be avoided by this

approach. A transition to an IPv6-only core could occur at a later time, when a sufficient amount of IPv6 applications are generating a significant amount of IPv6 traffic.

V. CONCLUSIONS AND RECOMMENDATIONS

A. ALLOCATION OF ADDRESS SPACE?

The Internet has provided the DoD the ability to exploit new theories that enable Net-centric warfare to become a reality. Net-centric warfare requires a culture change in relationships that will allow information sharing between various groups of people and organizations. The capabilities that Net-centric warfare introduces are on the cutting edge of technology and will enable commanders to dominate conflicts with greater precision. Commanders today have near real-time imaging of targets with photos and coordinates, which are transmitted by e-mail to aircraft in flight. Previously, commanders relied on maps, grease pencils, and radio reports to plan their strikes. The advances in technology that make modern day warfare possible require additional IP address space resources. Management of transitioning to networks capable of supporting these advances will therefore be a significant challenge for the foreseeable future.

B. ADDRESSING PLAN FOR THE DOD

It is clear the DoD must function in a dual IPv4/IPv6 capacity when implementing IPv6. Operating in this capacity is essential to maintaining the relevance of currently fielded programs. Having the ability to operate in a dual capacity will facilitate the transition to IPv6 because systems will not be precluded from operation on a specified date. Setting an estimated transition date as a goal is imperative to success. However, if the DoD had directed a specific transition date, programs without adequate resources would be facing losses in operational service. This means a phased transition approach is needed to ensure the continued operation of currently used IPv4 systems in the field.

The DoD should use a decision making process that incorporates various stakeholders at all levels of operation. Everyone from the individual soldier to the general officers should be communicating their concerns and opinions for this transition. This open communication and dialogue enables problems to be identified before policy is directed and implemented. It is apparent that the DoD took into account many aspects when considering a phased transition.

The DoD should first convert core networks to IPv6 and then convert the access level networks and application hosts to IPv6. This will ensure the network will already be compliant when individual programs become compliant. This also enables the IPv4 applications to operate on the IPv6 core without complication. When all applications are running on the IPv6 core, the IPv4 traffic will discontinue.

C. NETWORKS

Networks with several security levels create many challenges in securing information in a Net-centric environment. Having networks separate will ensure information of different security levels are kept separate and free from intrusion. Failure to adhere to this philosophy will endanger the security and integrity of sensitive information during transition.

D. DOD NETWORK INFORMATION CENTER IPV6 ADDRESS MANAGEMENT

Having the right information at the right time is imperative to the decision making process. Limiting the information flow by not including key stakeholders will hinder DoD decision makers ability to set informed policy. Additional resources will be required when information is continually distorted before it reaches DoD leadership. For these reasons, it is recommended the DoD organize in a horizontal structure when establishing policy that affects stakeholders at every level within the DoD.

When allocating address space at the resource allocation level, the MIL NIC and Agency NICs should adopt a hierarchical process for submitting address space requirements. This will increase transition efficiency, because agencies applying for address space will be required to demonstrate a valid need. When Agency NICs gather enough requests for address space, they can request a single block of space from the MIL NIC. This process will decrease the workload at the MIL NIC, increase efficiency for allocating address space, and provide a higher level of confidence that the request for address space is validated. If the MIL NIC and Agency NICs attempted to institute a horizontal approach to allocating address space at the resource level internal strife between agencies could emerge. When organizations are competing for address space on the same level confusion will emerge and efficiency will decrease.

Success in transitioning to IPv6 will require continuing some practices currently being used with IPv4. These practices include allowing the DoD NICs to continue maintenance of DNS servers, zone files, and delegate subordinate zones for their respective forward DNS zones will ensure this support.

E. ESTIMATING COST TO TRANSITION POR SYSTEMS FROM IPV4 TO IPV6

Legacy systems should be transitioned using Technology Refresh or Software Block upgrade programs. These upgrades must be implemented with careful analysis of the effects on tactical network operations. Systems with sufficient throughput for current needs should be transitioned using their normal technology refresh/software upgrade schedules. The estimated cost can be projected using standard software and hardware estimating models such as Constructive Cost Model COCOMO for software development. Systems without sufficient throughput to support transition should be maintained as IPv4-only systems. If these systems are not planned for obsolescence within the mandated five year window then the waiver process must be followed and replacement systems identified for future upgrades to those GIG assets.

The cost to transition systems in development from IPv4-only to IPv4 and IPv6 capability will be driven by maturity of the design for the system. The insertion of already approved software and hardware products from the JITC APL can alleviate much of the additional cost. It is recommended that the government work with the affected contractors in order to estimate the cost of the transition. The government must also generate an Independent Cost Estimate (ICE) in order to gain a full appreciation for the additional funding required. Finally, the government needs to account for additional interoperability and certification testing required for the transition.

The Army Deputy Chief of Staff, G-8, Programs must consider all input gathered from the PEOs before allocating resources. When direction is set prior to a complete analysis, significant amounts of rework are generally required. The guidance to use technology refresh funding to accomplish a significant portion of the transition resulted in the "good enough drill," decision which eliminated the majority of funding for technology refresh of the BFAs. To further complicate this situation, Joint Command

and Control (JC2) is slated to replace Command and Control (C2) and the JC2 Program Manager has not provided any programmatic information for transition. Presently, the JC2 BFA has no funding associated with its IPv6 transition requirements.

F. BENEFIT TO THE DOD OF TRANSITION

1. Interoperability

Having warfighting information systems on a network where intelligence can be posted, accessed, and analyzed is the DoD's concept for being Net-centric. Net-centricity requires not only the ability to share data but also the ability to create it. Net-centricity will enable the soldier to discover access, integrate, correlate, and fuse information and data to support their operations. To fully realize the potential of Net-centric operations, people, organizations, process, information, and material must operate synergistically. Accordingly, the DoD should address the business-process redesign first and then focus on the people, organization, and information needed to implement the new processes. When transiting to IPv6, organizations will need to change the way information is shared between organizations. The change will likely amount to adopting an attitude of openness, or willingness to share information, rather than a need-to-know attitude, which may be possibly the largest cultural challenge for the DoD.

2. Improved End-to-End Security

Maintaining the security of DoD networks from intrusion is a major concern for the DoD. Without guaranteed end-to-end security, information can become vulnerable to hackers or other system attacks that seek to pilfer classified or sensitive information. IDSs ensure IPv6 networks are protected from intrusion because they block hackers from entering networks without required security encryption. Achieving this goal will require more work in the availability and quality of IDSs. The DoD must follow Japan's lead in IDSs development. Japan began developing IDSs prior to IPv6 transition. The United States is behind the power curve in developing IDS and must aggressively pursue development or networks will lack adequate security controls.

Properly implementing and continually monitoring IPv6s security features is required for safeguarding network information. SEND devices must be implemented to protect users when accessing databases on the network. SEND will ensure that both

points of access on both the sender and receiver end of network traffic is secure. Implementing QoS will ensure time critical information is prioritized so it reaches the commander in a timely fashion, allowing tactical or strategic advantage. Mobile IP and auto configuration must be utilized in order for soldiers on the move to access information. IPSec will monitor user access and safeguard information that is beyond their need to know. Complete end-to-end IPSec is a necessary aspect of a Net-centric architecture because in this environment, various users will have differing security levels. Achieving confidence in security will require implementation and monitoring of these aspects in addition to continually updating the network as new security devices become available.

3. Ease System Management Burdens

Within the next few years wireless devices will be available to every soldier on the battlefield. This increase in wireless devices will demand significant amounts of IP address spaces and keeping networks flexible and available will be challenging. Networks will need to be scalable to keep management tasks from becoming serious burdens that degrade network operations.

One important aspect of address space management that should be implemented is a centralized database for IP addresses. This will ease management burdens because updates can be preformed concurrently. The centralized database will also allow for greater accuracy and consistency, which will lead to less confusion when users are trying to access information. When individual soldiers are equipped with PDAs special considerations should apply. Auto-configuration will be essential for users who are on the move because they will require seamless access to other networks within the battle space. Failure to implement auto-configuration would require additional time and resources to acquire needed information. These resources may not be available in time critical situations.

G. ISSUES SURROUNDING DOD TRANSITION

The DoD's transition has been extended to FY16 in order to minimize transition cost by increasing the use of Technology Refresh programs., It is important that planned

and programmed systems be acquired with support for both IPv6 and IPv4. This includes ensuring that:

- The requirements for all DoD developed products include both IPv6 and IPv4 support.
- Commercial products selected include both IPv6 and IPv4 support.
- Coexistence strategies must be developed to ensure interoperability with legacy systems until the transition is complete.

H. MAINTAINING INTEROPERABILITY

Acquisition cycles and product lifetimes for DoD GIG assets are usually substantially longer than commercial technology cycles, particularly for tactical-level systems. The increased bandwidth requirement will make transition impractical for some handheld, man packed, and vehicle mounted systems. The assumption that legacy systems will be obsolete in five years or less is inconsistent with the current operational and fiscal environments. The systems currently in development and slated to replace legacy system are more often than not, delayed in development due to several factors such as technical challenges, funding shortfalls, cost overruns, and schedule delays. It is projected that the legacy system will be required in the field far longer than the projected five year time frame.

The assumption that the Army will obtain IPV6 Upgrade through FCS, WIN-T, and JTRS assumes total replacement of existing systems. This is unlikely to happen on known schedules. At least some legacy systems will be in the field for the foreseeable future. Current Force and Future Force systems must therefore be interoperable. All new systems fielded will be required to support both IPv4 and IPv6 protocols. It is recommended that DoD development systems be implemented in a fashion to facilitate easy changes to the IP protocol as it matures (i.e., a strongly layered architecture that separates the network/IP layer). It is critical that the implementation facilitate changing the protocol.

I. SECURITY ISSUES

Many of the security threats to today's IPv4 networks will not disappear with the deployment of IPv6. This includes vulnerabilities present in higher level protocols and services within the network. There is an increasing emphasis on encryption technologies

which operate at the IP layer. As the DoD moves toward IPv6, these devices will need to be upgraded to support the new protocol. In the interim, tunneling architectures will have to be developed to support the use of IPv4 encryptors across IPv6 networks and vice-versa. The IPv4 encryptors may require software updates to implement tunneling.

J. IPV6 STANDARDS AND PRODUCT EVOLUTION

The current mandate by OSD is that all DoD PMs purchase from the JITC APL first. If a candidate product is not on APL, the product can be nominated for APL testing and certification. It is critical that PMs constantly monitor the APL in order to determine the progress with IPv6 standards and ensure the COTS products that are being integrated in their systems are certified and on the APL.

K. TESTING AND CERTIFICATION ISSUES

The DoD must generate an integrated T&E strategy to address the performance and scalability of IPv6 in networks. All IPv6 capabilities including, interoperability, transition techniques, and security solutions must be tested on these networks at the DoD level. This integrated T&E is needed to ensure that performance in secure environments using these IPv6 solutions still meets the user's operational requirements. Since IPv4 and IPv6 devices are expected to coexist for some time, thorough testing of interoperability, security, and performance is also critical for a smooth transition to IPv6.

L. RECOMMENDED DOD TRANSITION MECHANISMS AND STRATEGIES REGARDING IPV6

Given that legacy systems will be operational longer then advertised and because objective systems currently in development are often delayed, legacy systems will be utilized far longer then the projected five year time frame. PMs must accordingly incorporate acquisition strategies systems support IPv4/IPv6 interoperability throughout the system's lifecycle.

M. TRANSITION TRADE ANALYSIS CONSIDERATIONS

The PM should conduct transition trade analysis in order to assess transition scenarios and provide the best transition recommendations based upon each system's capability, logistics and schedule. Maturity of transition mechanisms and maturity of IP

devices on each system must be considered. The key parameters of the trade space seem to involve when the system transitions during its lifecycle and to what the system transitions.

N. PRE-DEPLOYMENT TRANSITION

For systems in development, the baseline design must be changed from an IPv4-capable to an IPv4/IPv6-capable system during the design phase. The focus of the pre-deployment transition analysis should center on the hardware ramifications and network architecture options including dual stacks, tunneling, and translation.

1. Dual Stack

The preferred method for DoD and commercial Internet networks is to deploy dual stack systems. The benefit of dual stack is design simplicity, but it requires extra software, memory and processing power within every device. Native IPv6 is less bandwidth efficient than IPv4 due to additional header size and optional header extensions. Additionally, the optimum size for Minimum Transmission Unit (MTU), fragmented packets, must be determined by detailed analysis and testing.

2. Tunneling

Some of the major issues for IPv6 tunnels IPv6 are that some require manual configuration. Since it uses IPv4 routing (not improved IPv6 routing), it cannot traverse IPv4 NATs (i.e. network address translation devices), and must be deployed with a tunnel broker service to automate setup and take down, and it may cause 20 or more packets to establish a tunnel (not useful for short data transfers). Configured tunnels may not be effective in tactical networks due to manual intervention, performance, and security. For this reason it is recommended that dual stack transition be implemented whenever technically feasible.

3. Translation

Each translation mechanism has its own advantages and disadvantages with respect to performance, security, operational efficiency, and scalability. However, each method requires either extra software within a host or an external device to provide this capability. Translation has high system overhead, limited manageability, is focused on a single host or single communications path, may have security limitations, and is a high-

cost alternative. Therefore, translation may not represent a viable alternative and should only be used as a last resort when both dual stack and tunneling are not technically feasible.

O. RECOMMENDED PRE-DEPLOYMENT TRANSITION MECHANISMS

Dual stack is the preferred mechanism because of its scalability and minimal impact on performance. It also meets current tactical network criteria for configuration, manageability, reliability, scalability and security. Dual stack has the additional benefit of requiring less bandwidth since it requires minimal connection setup.

When some portions of the tactical network do not support both IPv4 and IPv6, tunneling or translation may be required. The preferred method in this instance would be tunneling since translation requires either extra software within a host or an external device driving implementation cost. The extra burden on bandwidth and long latencies must be considered when implementing tunneling transition mechanisms.

P. POST-DEPLOYMENT TRANSITION

PMs should plan for transition using Technology Refresh or Software Block upgrade programs. The current force systems will be in the field for the foreseeable future. Current Force and Future Force systems will have to be interoperable. The one major issue with this approach is adequate IPv4 address space to accommodate the Dual stack IPv4/IPv6 environment.

Numerous tactical systems will remain IPv4 capable into the foreseeable future. Implementing a dual stack core and gradually execution of dual stack IPv4/IPv6 devices is the recommended approach. These devices and applications would attempt to “favor” IPv6 but have the ability to fall back on IPv4 as a secondary method. Traffic would be carried end-to-end as either IPv6 or IPv4 whenever practical. This approach could potentially avoid the use of many transition mechanisms, which themselves introduce a great deal of complexity. Additionally, many of the IPv6 transition mechanisms introduce single points of failure which could be avoided by this approach. A transition to an IPv6 only core could occur later, when a sufficient amount of IPv6 applications are generating a significant amount of IPv6 traffic.

Q. FINAL THOUGHTS

The critical areas PMs must address to ensure a smooth transition to IPv6:

- DoD GIG assets must function in a dual IPv4/IPv6 capacity when implementing transition to IPv6 in order to maintain the relevance of currently fielded programs.
- Maintaining separate networks for different security levels will ensure information security and keep networks free from intrusion.
- The DoD should organize in a horizontal structure when establishing policy that affects stakeholders at every level within the DoD.
- Legacy GIG assets should be transitioned using Technology Refresh or Software Block upgrade programs. Upgrades must be implemented with careful analysis and testing in order to determine the effects on tactical network operations and the performance of these assets.
- GIG assets in development must transition from IPv4-only to IPv4 and IPv6 capability.
- The OSD mandate is that all DoD PMs purchase from the JITC APL first. If a candidate product is not on APL, the product can be nominated for APL testing and certification.
- Since IPv4 and IPv6 devices are expected to co-exist for some time, thorough testing of interoperability, security, and performance is critical for a smooth transition to IPv6.
- PMs should conduct transition trade analysis in order provide the best transition approach based upon each GIG asset's capability, logistics and schedule.
- Pre-Deployment transitions should utilize the Dual stack transition mechanism due to its scalability and minimal impact on performance.

LIST OF REFERENCES

1. Department of the Army Internet Protocol Version 6 (IPv6) Transition Plan (Phase 1) Version 0.9, 11 March 2004.

2. Brig, P. Michael and Cansever, Derya. An IPv6 Unicast Addressing Plan for the DoD Rev 1.0 (Alternate): February 6, 2006.

3. DoD CIO Memo - Internet Protocol Version 6 (IPv6) http://www.dod.mil/nii/org/cio/doc/IPV6.pdf June 9, 2003 ASD(NII)/DoD CIO. Last accessed September 2006.

4. DoD CIO Memo - Internet Protocol Version 6 (IPv6) Interim Transition Guidance http://ipv6.disa.mil/docs/stenbit-ipv6-guidance-20030929.pdf 9/29/2003 ASD(NII)/DoD CIO. Last accessed September 2006.

5. Army CIO/G6 Memo – Army Implementation of DoD Internet Protocol Version 6 (IPv6) Mandate https://www.us.army.mil/suite/portal/index.jsp 11/5/2003 Army CIO/G6. Last accessed October 2006.

6. Department of the Army Additional Guidance Memo on IPv6-FY08 Goal, Including Enclosure 1 https://www.us.army.mil/suite/portal/index.jsp 4/1/2004 Army CIO/G6. Last accessed October 2006.

7. The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan Version 2, June 2006 ASD(NII)/DoD CIO.

8. Army IPv6 Transition Plan https://www.us.army.mil/suite/portal/index.jsp Version 1.0 (Draft), September 15, 2004 Army CIO/G6 –IPTWG. Last accessed October 2006.

9. DoD Information Technology Standards Registry (DISR) https://disronline.disa.mil/a/DISR/DISR_reports.jsp Release 06-2.0 / June 27, 2006 DISA. Last accessed October 2006.

10. DoD IPv6 Standard Profiles for IPv6 Capable Products Mandated: https://disronline.disa.mil/a/DISR/view_kip_family.jsp?spId=807 Emerging: https://disronline.disa.mil/a/DISR/view_kip_family.jsp?spId=807 Version 1.0 / June 1, 2006 DISA-ITSG. Last accessed October 2006.

11. DoD Master Test Plan Version 2/June, 2006 ASD(NII)/DoD CIO - DITO.

12. DoD IPv6 Generic Test Plan http://jitc.fhu.disa.mil/adv_ip/register/register.html Continuously Updated JITC. Last accessed November 2006.

13. JITC IPv6 Interoperability Certification Process http://jitc.fhu.disa.mil/adv_ip/register/register.html Continuously Updated JITC. Last accessed November 2006.

14. IPv6 APL Test schedule http://jitc.fhu.disa.mil/adv_ip/register/register.html Continuously Updated JITC. Last accessed November 2006.

15. DoD IPv6 Test and Evaluation Working Group (TEWG) Charter 12/12/2005 DISA-ITSG.

16. DoD IPv6 Transition Steering Group (ITSG) Charter 8/5/2006 ASD(NII)/DoD CIO - DITO.

17. The Fiscal Year 2006 Department of Defense Internet Protocol Version 6 Test and Evaluation Report dated September 2006.

18. Director, Technical Architecture Division Architecture Operations Network & Space CIO/G-6.

19. Implementers IPv6 Transition Plan for PEO Ground Combat Systems.

20. IPv6 Transition Guidance Federal CIO Council Architecture and Infrastructure Committee February 2006.

21. Implementer Ipv6 Transition Plan for Program Executive Office Command, Control, and Communications Tactical (PEO C3T) dated 24 May 2004

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California